AlterPath KVM/net Manual

A reference guide for users and systems administrators of Cyclades AlterPath KVM/net

Product Version 1.0.0
Document Revision 6

We believe the information in this manual is accurate and reliable. However, we assume no responsibility, financial or otherwise, for any consequences of the use of this product or manual. This manual is published by Cyclades Corporation, which reserves the right to make improvements or changes in the products described in this manual as well as to revise this publication at any time and without notice to any person of such revision or change. All brand and product names mentioned in this publication are trademarks or registered trademarks of their respective holders.

For latest manual revisions, please refer to Cyclades website on:
http://www.cyclades.com/support/downloads.php

Table of Contents

Before You Begin

Chapter 1: Introduction

Chapter 2: KVM/net Installation

Chapter 3: KVM/net Configuration

Chapter 4: KVM/net Operation

Before You Begin

Welcome to the AlterPath KVM/net Manual! This manual is designed to guide you in installing, configuring, and operating AlterPath KVM/net, as well as other necessary information to guide you in your day-to-day operations of the product.

Audience

This manual is intended for System administrators and regular users of AlterPath KVM/net. The regular user is expected to have a basic knowledge of using a graphical user interface such as MS windows or a web browser.

Document Organization

The document is organized as follows:

1: Introduction — Defines and explains the overall product features and uses of KVM/net.

2: KVM/net Installation — Explains the procedure for installing and setting up KVM/net.

3: KVM/net Configuration — Explains how to use the user interface, highlighting such procedures as how to configure the KVM/net switch, adding or deleting users, defining user access, adding or deleting server connections, and other topics pertaining to KVM/net administration.

4: KVM/net Operation — Presents the procedures for connecting to a port and other operations related to using the web user interface.

Appendix A: — Technical Specifications

Glossary

This is a glossary of terms and acronyms used in the manual.

Typographical Conventions

Screen Labels

Words that appears on the screen are typed in **boldface**.

Examples: The **Configuration** window; the **Password** field.

Hypertext Links

With the exception of headings and the Table of Contents (which are already linked), all <u>underlined</u> words are hypertext links.

Important words

Certain words are *italicized* for emphasis.

Screen Levels

Screen levels are indicated by the "greater than" symbol (>), starting from parent to child to grandchild and so forth.

Example: **Main Menu** > **Configure** > **User Configuration**

Untitled Data Fields

Some data entry fields of the GUI windows or forms do not have titles. When this field is described in any field definition section of the manual, the field is indicated as either untitled or by its GUI type, and enclosed in angled brackets.

Examples:
[*untitled*] Type in the port number in this field.
[*view table*] Select the user from the view table.

Untitled forms

While most forms are identified by it's menu selection, some forms do not bear the title. The manual uses initial capitals to refer to their names or titles.

Examples:
The Data Buffering form; the VPN Connections form; the Active Ports Session form.

User entry words

Words or characters that you would type in are shown in `courier`.

Example: `myPas8worD`

Naming Conventions

Form

The form is the largest part of the user interface; it contains the user selection or input fields for each selected item in the menu.

Form Names

The form names of the web user interface do not necessarily appear on the actual window. Because some forms do not have titles, these names are used to distinguish each form as well as to reflect the form function.

KVM/net

Short name for AlterPath KVM/net. This manual uses both terms to refer to the KVM/net switch or unit or as a product line.

Select

To *select* is the same as to *click your mouse*.

Symbols

This manual uses three symbols to indicate the following:

📚 This icon indicates a reference to another section, chapter, or document.

📝 This icon indicates a note or comment.

💻 This icon indicates a warning.

This page has been left intentionally blank.

Chapter 1
Introduction

Cyclades AlterPath™ KVM/net is a family of keyboard-video-mouse switches designed to provide you with full access and control of servers or computers across your network over the internet. Being also CAT-based, the KVM/net at once offers a simple and secure way to manage remote servers either locally (up to a distance of 500 feet) or remotely, through a standard internet browser[1] from anywhere in the world.

The KVM/net provides two types of web user interface:

- Web configuration interface (for administrators)
- Web user interface (for regular users)

KVM/net provides all the conveniences and features of a well-integrated KVM switch. Using KVM/net, you can access GUI-based servers (*e.g.*, Windows NT or Windows Server 2003) through a dedicated channel or over the network.

The flexibility of CAT5 cabling (supporting distances of up to 500 feet between the switch and the managed servers) enables KVM/net to use any data center's existing cabling infrastructure, providing for an easy installation.

Its security features allow KVM/net to be integrated with existing security infrastructure such as RADIUS, TACACS+, LDAP and Kerberos, as well as token-based strong authentication methods such as SecurID. As backup, KVM/net also provides local authentication should any of the authentication servers fail.

Cascadeable to 1024 servers, cascading support with centralized port management allows KVM/net to increase the number of managed servers without losing the initial investment or the advantage of centralized configuration and access interface. This allows data center managers to expand their coverage as the data center grows.

[1] The internet browser and Java plug-in currently supported by AlterPath KVM/net are **Internet Explorer 6.0** and **Java 2 Runtime Environment (JRE) SE v1.4.2**.

Connectivity and Server Capacity

KVM/net supports two concurrent users, one remote and one local.

For one AlterPath KVM/net16 master, you can connect up to eight KVM units as slaves; and for one AlterPath KVM/net32, up to 16 KVM units as slaves. Two connections are used for each slave-to-master configuration to allow two simultaneous users. One CAT-5 cable between a master port to a slave USER 2 port and another CAT 5 cable between a master port and a USER 1 port through a terminator.

Through cascading, using one port per slave, AlterPath KVM/net allows you to control up to1024 servers from a single KVM/net console -- either locally or over the Internet Protocol.

Product Components

AlterPath KVM/net family comprises four product components:

- AlterPath KVM/net 16 - model that comes with 16 KVM ports.
- AlterPath KVM/net 32 - model that comes with 32 KVM ports.
- AlterPath KVM RP - allows a remote user to connect to the KVM/net.
- AlterPath KVM Terminator - interfaces the console keyboard, video and mouse to the KVM/net.

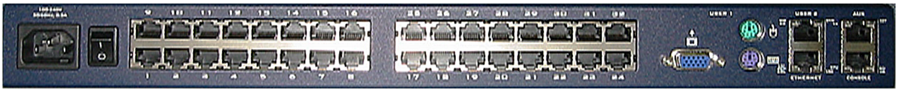


Figure 1.1 - AlterPath KVM/net 32: Back View

Overview of AlterPath KVM/net

The KVM/net operates by using the keyboard, VGA, and mouse as the low-level access interfaces to the managed servers, enabling you to access server information that is otherwise inaccessible through in-band network interfaces.

For example, BIOS access, POST and boot messages are inaccessible through in-band network interfaces. Such information becomes available only after the system boot is completed.

In some cases, the in-band network interfaces are not available even after the system boot is completed (*e.g.*, after a Windows Safe Mode boot), making the KVM/net interface the only way to manage remote, GUI-based servers.

KVM/net offers advanced options to meet the most demanding user requirements. It provides two types of web interface: configuration and user interface, cascading support, CAT5-based cabling for up to 500 feet of distance and integration with other server management devices such as the AlterPath PM IPDUs are some of the options that provide the flexibility necessary for the AlterPath™ KVM/net to fit into most customer applications.

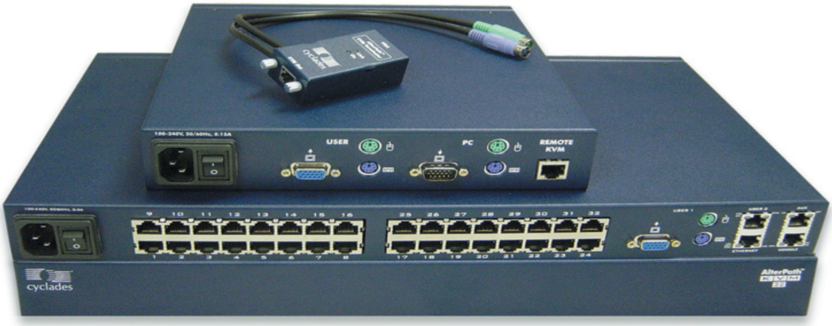


Figure 1.2 - AlterPath KVM/net Product Suite
(From bottom: KVM/net unit, front; KVM/net 32 unit, back; KVM RP; KVM Terminator.)

KVM/net Product Features

AlterPath KVM/net provides enterprise solutions, meeting the needs of today's data center. Among the most notable features of AlterPath KVM/net are:

- Web Configuration and Operation Interface
- CAT5-based cabling
- Server-Based Authentication
- Local User Authentication
- User Access List Per Port
- Cascading Support with Centralized Port Management
- Flexibility and Scalability
- Online Screen Display
- Mouse Support
- Multi-User
- Event Logging
- Linux Advantage
- Rack Space Savings

Remote Access Over IP

KVM/net provide users the advantage of accessing servers from any place at any time by enabling full access and server control over the Internet Protocol. Unlike an analog KVM switch, this feature does away with the need for physical access to the console controlling the connected servers to that switch, and allows the user to control the servers using a standard web browser[1].

Web User Interface for Configuration and Operation

The KVM/net offers two types of web graphical user interface:

- **Configuration** - Using the web configuration interface, KVM/net provides a full complement of windows and forms to enable the system administrator full and complete configuration of the KVM/net system and its users.
- **Operation** - Using the web user interface, the regular user can launch the AlterPath viewer to connect to servers and to manage

[1] The currently supported browser is **Internet Explorer 6.0**.

them rapidly and easily. The same GUI functions enable power management that allows them to control IPDUs associated with the KVM/net.

Cat5-Based Cabling

Ethernet LAN connection aside, CAT5-based cabling allows for a clean cabling setup and access to servers located far away from the AlterPath KVM/net switch. CAT5 cabling allows you to use existing cabling infrastructure in the data center, making system setup quick and simple. The KVM/net supports distances up to 500 feet between the switch and the managed servers, making even the most remote server in the data center reachable by the AlterPath KVM/net.

Server-Based Authentication

AlterPath KVM/net supports RADIUS, TACACS+, LDAP and Kerberos, as well as token-based strong authentication methods such as SecurID, which allows it to provide a high level of security and adapt to your current security policies and infrastructure.

For example, in large data centers with hundreds of KVM switches that support user authentication using locally-stored passwords, each time a new user is created or removed, the system administrator has to manually reconfigure each device. Security is compromised if he forgets or misconfigures any device. With server-based authentication, the administrator updates a single centralized database and all access devices consult that database using RADIUS or LDAP.

Local User Authentication

AlterPath KVM/net also supports local backup user authentication, allowing the system to fall back to local authentication mode in case your server-based authentication engine is unreachable. This ensures continuous, secured access to your servers, even if the network or the authentication server is down.

User Access Lists Per Port

This feature allows you to define which users have access to which servers, providing greater control and peace of mind.

Cascading Support with Centralized Port Management

You can have multiple AlterPath KVM/net switches cascaded to provide higher port density, yet they will behave as one single, larger KVM switch. This means that you can configure the entire KVM/net switch chain from a single point (the master unit). Once it's ready, it is broadcasted to all the units in the chain, considerably simplifying the configuration process.

User authentication and access follows the same approach, which means you authenticate only once and choose the server you want to access from a single list, and the AlterPath KVM/net chain will automatically connect you to the proper server.

Flexibility and Scalability

Cascading support with centralized port management allows the KVM/net to increase the number of managed servers without losing the initial investment, or the advantage of a centralized configuration and access interface. As the data center grows, managers and system administrators have greater control, and the ability to expand their coverage.

On-Screen Display Capability

You can use the on-screen display (or the AlterPath Viewer) to control your AlterPath KVM/net easily. From the OSD, you can perform tasks such as navigating through the servers, cycling servers, and so forth.

Mouse Support

AlterPath KVM/net currently supports the PS/2 mouse. In the future, it will support USB and Sun mouse models.

Multi-User

KVM/net supports two concurrent users; one local (which is extendable to 500 feet through the use of a CAT5 cable) and one remote *(i.e.*, over the internet). The KVM/net RP enables the remote operator to select the local keyboard, video, and mouse console between a local station and a server from the AlterPath KVM/net.

Event Logging Capabilities

AlterPath KVM/net provides event logging capabilities, allowing your organization to audit its usage and identify who accessed which KVM/net ports at what time and date. This helps your organization track how server issues are being handled by systems administrators, and analyze problem-solving policies for future improvement.

Linux Advantage

Instead of using proprietary software technologies, KVM/net leverages on Open Source software (Linux), giving users the freedom to customize its operation, to modify or add features.

Rack Space Convenience

Available in 16 and 32-port models that fit in 1U of rack space, KVM/net helps maximize server availability with scalability and security. Using KVM/net for server management decreases network maintenance costs while increasing efficiency and productivity.

Setup Diagram

The diagram below shows how the various KVM/net product components are connected and set up.

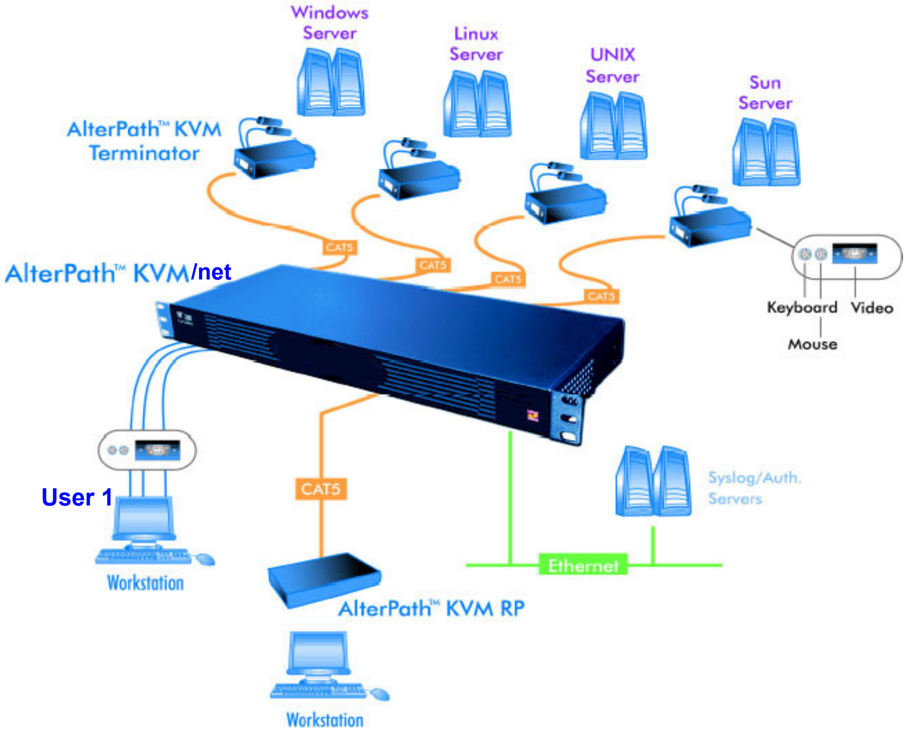


Figure 1.3 - AlterPath KVM/net Setup

Chapter 2

KVM/net Installation

This section discusses the procedures and requirements for installing the AlterPath KVM/net, and is organized as follows:

- Product Installation Checklist
- Rack Mounting and Connecting the KVM/net Components
- Installing AlterPath KVM/net
- Cascading AlterPath KVM/net

Product Installation Checklist

While the quantity of the product components may vary based on your order, at a minimum, your AlterPath KVM/net package should contain the following items:

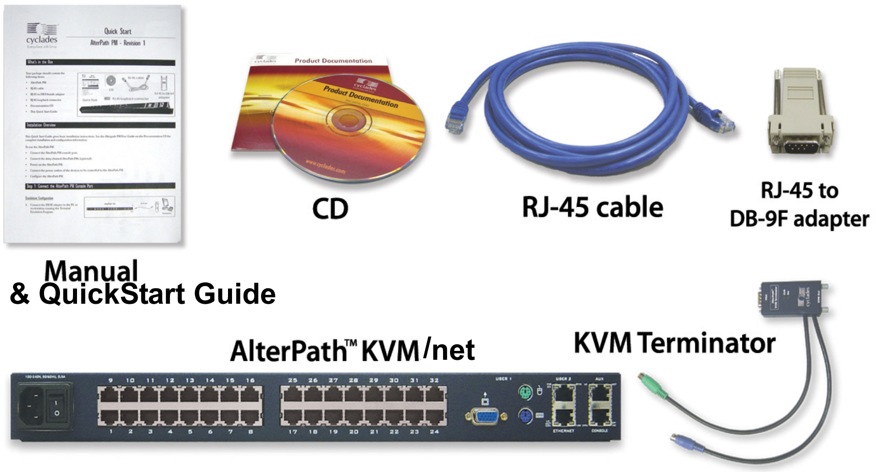
- 1 AlterPath KVM/net
- AlterPath KVM Terminator[1]
- 1 RJ-45 straight-through cable
- 1 RJ-45 to DB-9F crossover adapter
- 1 Power cable
- 1 Rack mounting kit
- 1 Manual
- 1 Quick Start Guide

Your AlterPath KVM RP should contain the following items:

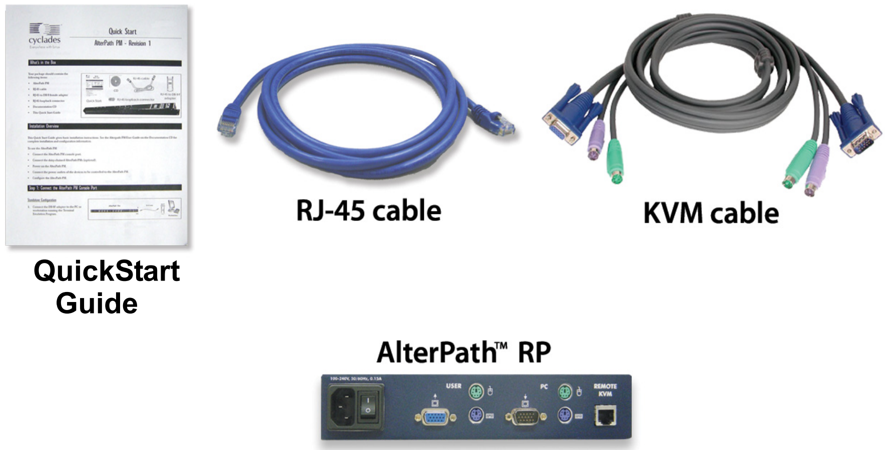
- 1 AlterPath KVM RP
- 1 RJ-45 straight-through CAT5 cable
- 1 Power cable
- 1 KVM cable
- 1 Quick Start Guide

[1] This item is only included based on the customer’s need.

The contents of a typical AlterPath KVM/net package is shown below: (Power cord and mounting kit not shown.)



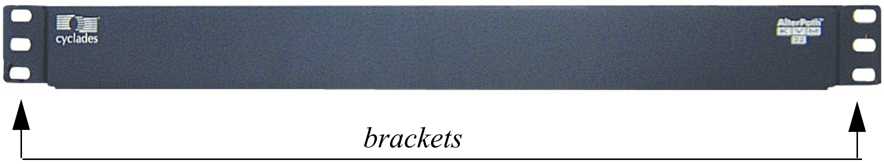
The contents of a typical AlterPath KVM RP package is shown below:



Rack Mounting and Connecting the KVM/net Components

To rack-mount and connect the KVM/net to your network, perform the following steps:

1. Install the brackets onto the front corners of the box using a screw driver and the screws and bolts provided with the rack mounting kit.

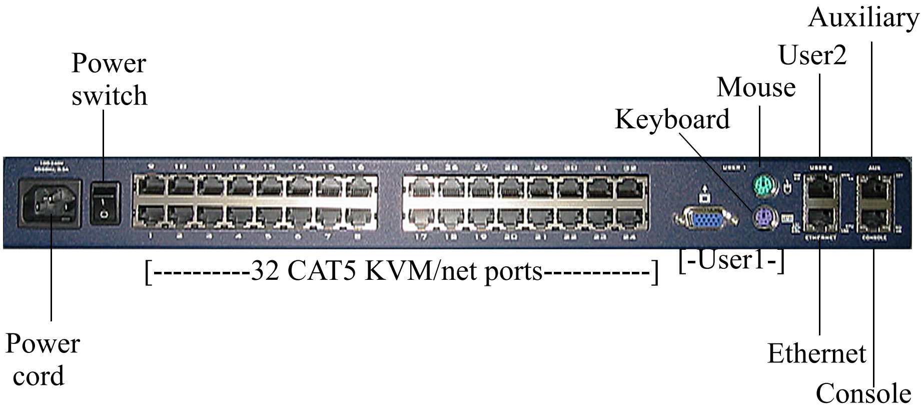


2. Mount the KVM/net box in a secure position.

   Refer to the **Safety Considerations When Rack Mounting** section of this chapter to ensure safety.

Port Connections

The diagram below shows the port connections located in the back of a KVM/net32:



Installing AlterPath KVM/net

While the KVM/net and its components are hot-pluggable, be aware that other non-Cyclades system components which are also connected may potentially stall your system. When in doubt, power on the KVM/net unit only after everything is installed properly.

To install your AlterPath KVM/net, follow the procedure below:

1. Connect computers to the AlterPath KVM/net.

   a. Select the appropriate KVM Terminator for the computer to be connected. Three Terminator types are available: PS/2, USB and Sun.

   b. Plug the selected Terminator to the matching Keyboard, Video and Mouse ports on the computer.

   When connecting the terminator, you must first connect the video, then the mouse, then the keyboard, before connecting the RJ-45 straight-through CAT5 cable.

   c. Repeat steps a and b for all computers to be connected.

   d. Plug RJ-45 straight cables from each terminator to the CAT5 ports on the AlterPath KVM/net.

2. Connect a local user station to the AlterPath KVM/net.

   a. Plug your station's Keyboard, Video and Mouse cables to the Keyboard, Video and Mouse **USER 1** connectors on your AlterPath KVM/net.

3. *Optional*. Connect the Remote Point Unit (RP) to the AlterPath KVM/net.

   a. If you are NOT using an AlterPath KVM RP, skip this and proceed to step 4.

   b. Plug your Keyboard, Video and Mouse to the Keyboard, Video and Mouse connectors on your AlterPath KVM RP.

d. Using the supplied KVM cable, plug your station's Keyboard, Video and Mouse to the Keyboard, Video and Mouse Local PC connectors on your AlterPath KVM RP.

e. Connect an RJ-45 straight cable from the REMOTE KVM port on the AlterPath KVM RP to the **USER 2** connector at the AlterPath KVM/net.

4. Power on your AlterPath KVM/net.

   a. Connect the AC power cable of the AlterPath KVM/net to the power connector of the unit. Make sure the power switch is off.

   b. Plug the other end of the cable to an AC wall power outlet.

   c. Power on your AlterPath KVM/net by turning its power switch on.

5. *Optional*. Power on your AlterPath KVM RP.

   If you have a workstation connected to your AlterPath KVM RP, power will be driven from the Keyboard interface on your workstation, and thus you can skip this step.

   a. Connect the AC power cable of the AlterPath KVM RP to the power connector of the unit. Make sure the power switch is off.

   b. Plug the other end of the cable to an AC wall power outlet.

   c. Power on your AlterPath KVM RP by turning its power switch on.

6. Power on the connected computers and proceed to Chapter 3: KVM/net Configuration.

Using Ethernet Connection

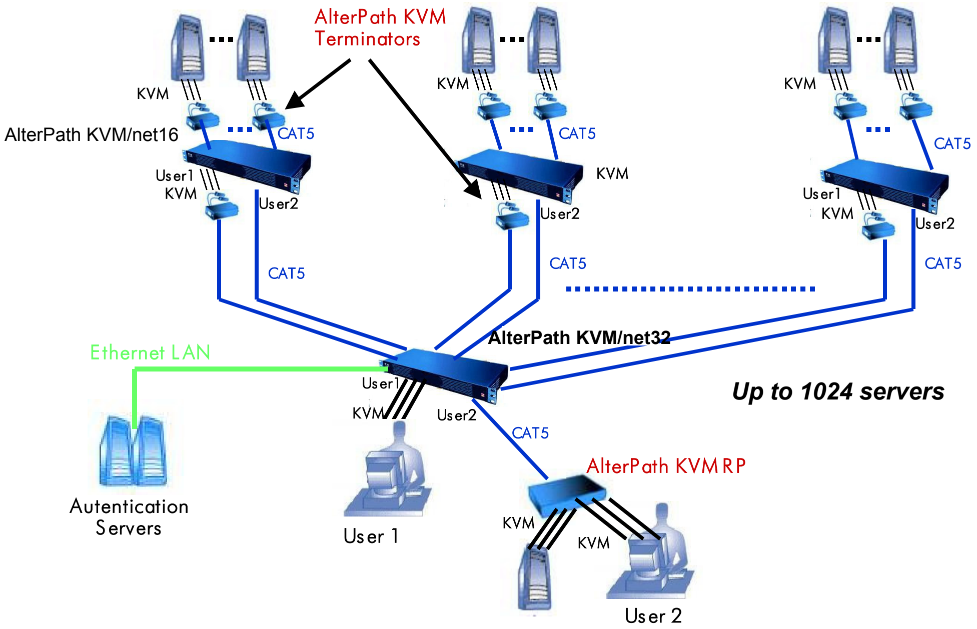
When you connect the ethernet port to your LAN, the KVM/net gets its IP address from your DHCP server automatically. Once KVM/net is assigned an IP address, any user on the network should be able to access the KVM/net through the web user interface.

Cascading AlterPath KVM/net

The AlterPath KVM/net is cascadeable to support up to 1024 computers. For one KVM/net 32 master, you can either connect up to 32 KVM32 units as slaves (2-user configuration), which enables control up to 512 servers; or up to 32 KVM32 units as slaves (single user configuration), which enables control up to 1024 servers.

The 2-user configuration uses two connections for each slave-to-master configuration. One CAT-5 cable between a master port to a slave USER 2 port and another CAT 5 cable between a master port and a USER 1 port through a Terminator. That is, for one user, you can use one port per slave; for two users, two ports per slave.

A typical cascading configuration is shown below:



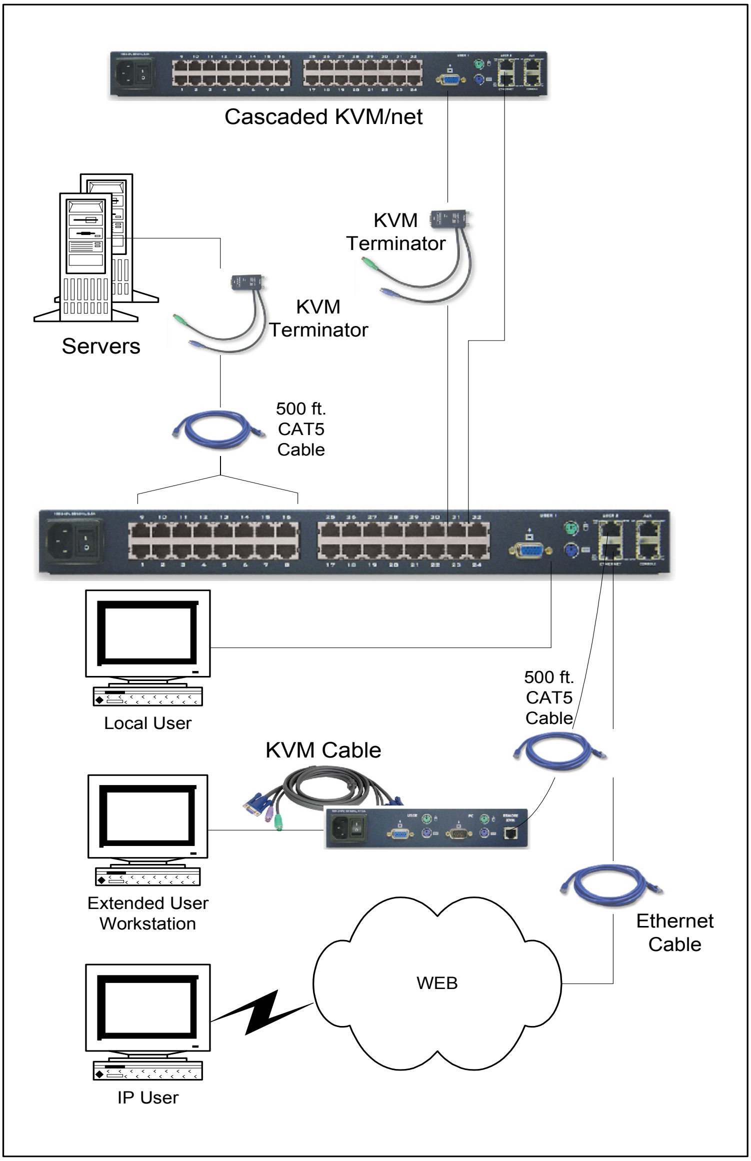
Connecting a Slave KVM to a Master KVM/net

The procedure for connecting a slave KVM to a master KVM/net is as follows:

1. Ensure that all hardware (KVM/net switches and computers) to be connected are switched off.
2. Connect a CAT5 cable from a master KVM/net port to the **USER2** (for remote station) port of the slave KVM.
3. Connect a KVM Terminator to the **USER1** (for local station) port of the slave KVM.
4. Connect CAT5 cable from a master KVM/net port to the KVM Terminator connected to the slave KVM USER1 port.
5. Repeat steps 1 through 4 for each slave KVM to be connected to the master KVM/net.

KVM/net components and connections

Below is a schematic diagram of the KVM/net components and connections as discussed in the installation procedure.



Safety Considerations When Rack Mounting

When rack-mounting the KVM/net box, consider the following:

Operating Temperature

The manufacturer's recommended operating temperature for the KVM/net is 50° to 112°F (10°C to 44°C).

Elevated operating ambient temperature

If you install the KVM/net in a closed or multi-rack assembly, the operating ambient temperature of the rack environment may be greater than the room ambient temperature. Ensure that you install the equipment in an environment compatible with the manufacturer's maximum rated ambient temperature.

Reduced air flow

Ensure that the amount of airflow required for safe operation is not compromised.

Mechanical loading

Ensure that the equipment mounted or loaded evenly to prevent a potentially hazardous condition.

Circuit loading

Ensure that the connection of the equipment to the supply circuit and the effect that overloading of circuits might have on overcurrent protection and supply wiring. Check the equipment nameplate ratings to address this concern.

Reliable Earthing

Maintain reliable earthing of rack mounted equipment by inspecting supply connections other than direct connections to the branch circuit such as power strips or extension cords.

This page has been left intentionally blank.

Chapter 3
KVM/net Configuration

This chapter presents the procedures for configuring the KVM/net using the web interface, and is organized as follows:

Overview

Configuring the KVM/net through the web configuration interface is the responsibility of the system administrator. This chapter is addressed to the System Administrator who is responsible for configuring and managing the KVM/net and its users, as well as to those users who are granted administrative access to configure and operate the KVM/net.

While the main focus of this chapter is on the use of the KVM/net web interface, it also presents a few configuration procedures using VI or the Command Line Interface (CLI), as necessary.

The KVM/net web configuration interface provides two modes of operation: Wizard and Expert. The organization of the chapter follows, in sequential fashion, the two modes and the menu selections available from each mode.

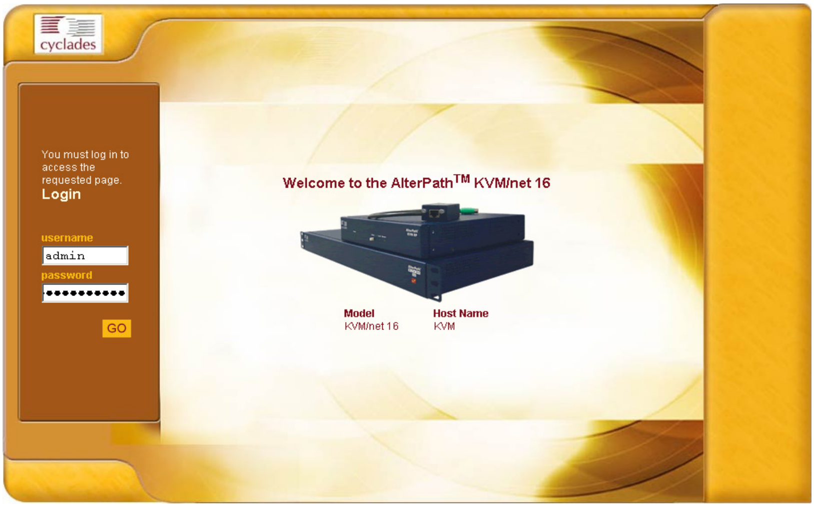
*If you are a regular user, refer to **Chapter 4: KVM/net Operation**.*

Logging In

IMPORTANT: *Take note of this login procedure. All subsequent online procedures in this chapter will assume that you are already logged in.*

1. Connect your internet browser to the KVM/net web interface by typing in the KVM/net server's IP address (*e.g.*, http://10.0.0.0) in the browser's address (URL) field.

   The system brings up the AlterPath KVM/net Login page:



You must log in to access the requested page.

Login

username: admin

password: ●●●●●●●●●●●

Welcome to the AlterPath^{TM} KVM/net 16

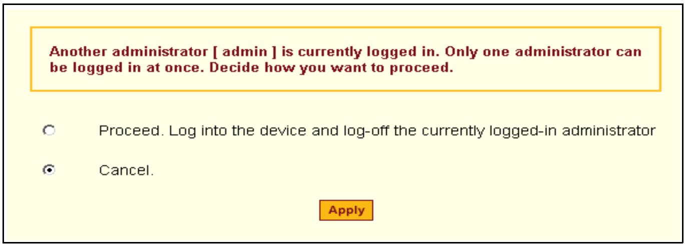
Model: KVM/net 16

Host Name: KVM

2. Log in as **admin** and type in the password: **cyclades**

   The system brings up the KVM/net web management page.

   If another administrator is using the system, the following message appears:



Another administrator [admin] is currently logged in. Only one administrator can be logged in at once. Decide how you want to proceed.

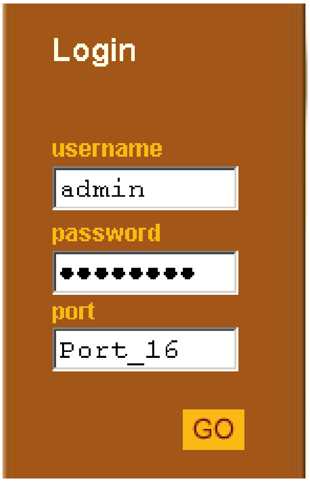
○ Proceed. Log into the device and log-off the currently logged-in administrator

● Cancel.

3. Click on the appropriate radio button and then click on the **Apply** button.

Direct Access to a Port

If the Login page is configured to allow Direct Access to a port, then a third field, **port**, should appear on the **Login** panel of the **Login** screen.



Login

username

admin

password

●●●●●●●●●

port

Port_16

1. From the port field, enter the port alias or the port number using the following format: **Port**_[number]

   Example: **Port_4**

2. Click on GO.

   The system connects you to the port.

KVM/net Web Management Interface

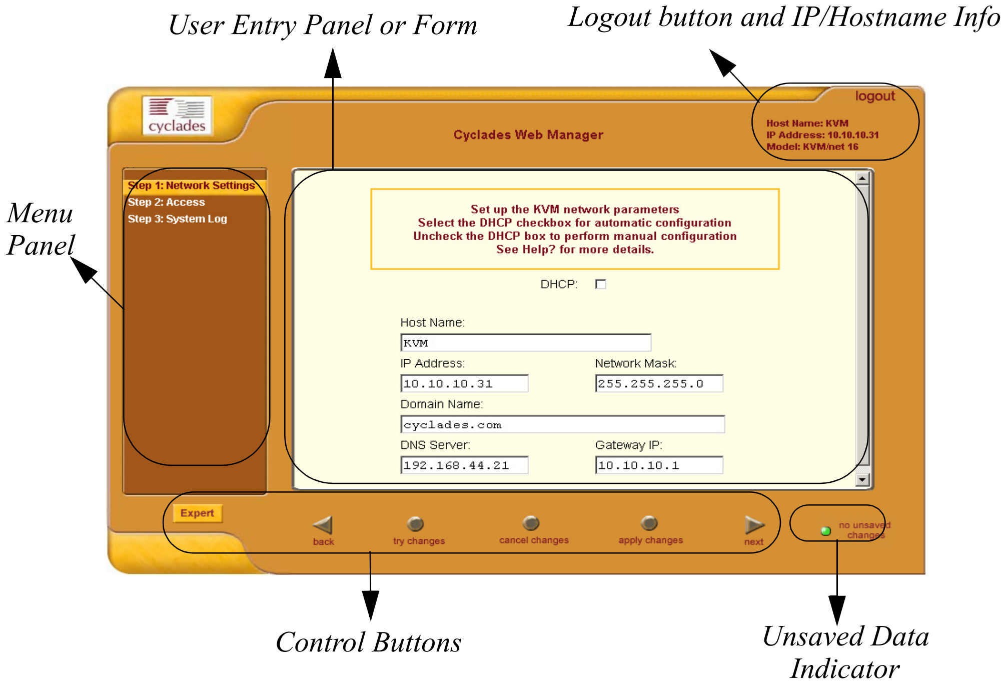
You can use the KVM/net web management interface in two modes:

- Wizard
- Expert

Wizard Mode

The wizard is an intelligent system that simplifies configuration by providing users the default parameter values, prompting you for only the necessary fields, giving specific instructions during the process and, in some cases, populating the fields automatically.

The Wizard Mode allows you to perform the basic configuration necessary to set up KVM/net and users in the quickest possible way. When you log on to KVM/net the first time, the system, by default, is in the Expert Mode. Make sure you select the **Wizard** button located at the bottom of the Menu Panel the first time you configure the web management interface.



Host Name: KVM
IP Address: 10.10.10.31
Model: KVM/net 16

Set up the KVM network parameters
Select the DHCP checkbox for automatic configuration
Uncheck the DHCP box to perform manual configuration
See Help? for more details.

DHCP: □

Host Name: KVM

IP Address: 10.10.10.31

Network Mask: 255.255.255.0

Domain Name: cyclades.com

DNS Server: 192.168.44.21

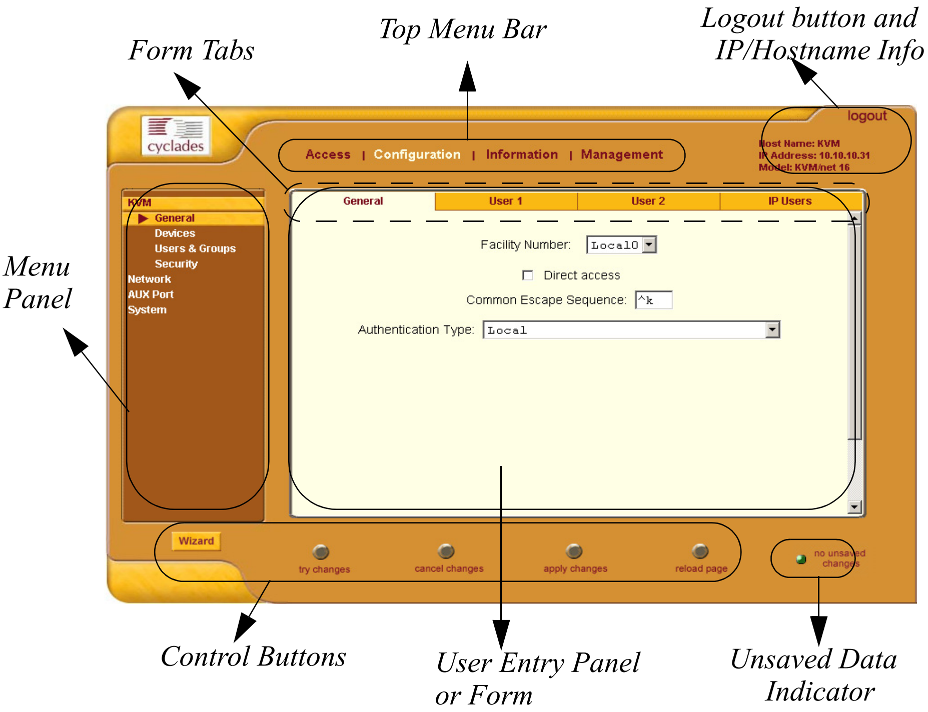
Gateway IP: 10.10.10.1

Shown in the previous page is a *typical* configuration window of the KVM/net web interface in Wizard Mode. The user entry panel or form varies depending on the selected menu item. The KVM/net uses forms and dialog boxes (*i.e.*, pop-up windows that prompt you for information) to receive your data input.

As mentioned, the web interface always starts from the Expert Mode. To configure in Wizard Mode, you must select the **Wizard** button.

Expert Mode

Designed for advanced configuration, clicking the **Expert** button at the bottom of the menu panel switches the web interface from Wizard to Expert Mode. Shown below is a typical (but not necessarily the first) KVM/net screen in Expert Mode. One main difference between the two modes is that in the Expert Mode you will notice the addition of a top menu bar to support a wider array of menu choices.



Host Name: KVM
IP Address: 10.10.10.31
Model: KVM/net 16

Facility Number: Local0

□ Direct access

Common Escape Sequence: ^k

Authentication Type: Local

The top menu bar supercedes the left menu panel. Based on what you select from the top menu bar, the left menu selections will change accordingly.

Occasionally, an Expert Mode menu selection will comprise multiple forms such as the one shown above. These forms are identified by their tabs. Select the tab to access the form that you want.

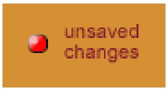
Button Functions

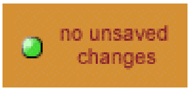
The control buttons located at the bottom of the KVM/net Web Configuration window provide you the following functions for operating the interface.

Button Name	*Use this button to:*
Wizard / Expert	Switch the KVM/net Web Configuration Screen to either Wizard or Expert Mode. The Expert Mode is the default mode; in this mode, the Wizard button is visible and vice versa.
Try Changes	Test or run the system based on the settings from the current form without having to save the configuration.
Cancel Changes	Cancel your changes or reverts back to the original configuration values.
Apply Changes	Save your changes to the KVM/net Flash card.
Reload Page	Reloads or refreshes the current page.
Next	Traverse to the next screen or form.
Back	Return to the previous screen or form.
Help?	Invoke the online help sub window which provides help information relating to the current form.

Saving Your Configuration

The **Unsaved Changes** indicator on the lower right hand corner of the KVM/net web configuration window serves to remind you that you have made a configuration entry or change which has not been saved.





Unless you do not need to save your configuration, be sure to select the **Apply Changes** button to save your configuration to Flash.

Configuring in Wizard Mode

As shown in the menu, the Wizard Mode configuration is composed of three steps:

Step 1: Network Settings

Step 2: Access

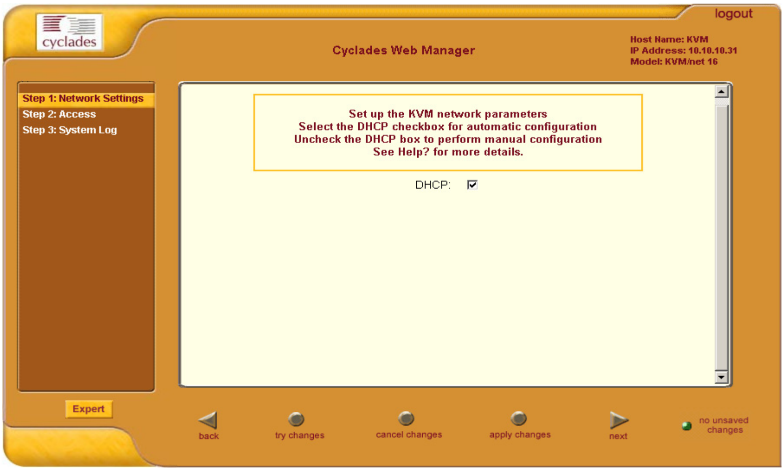
Step 3: System Log

Step 1: Network Settings

The Network Settings enable the entire system to recognize the KVM/net and its connection to the network. To configure the network settings for the KVM/net, follow the following steps:

1. From the main menu of the web interface, select **Step 1: Network Settings.**

   The system brings up the DHCP page (shown below). By default, the DHCP checkbox is check marked, which means that the system is already configured to use the DHCP server.



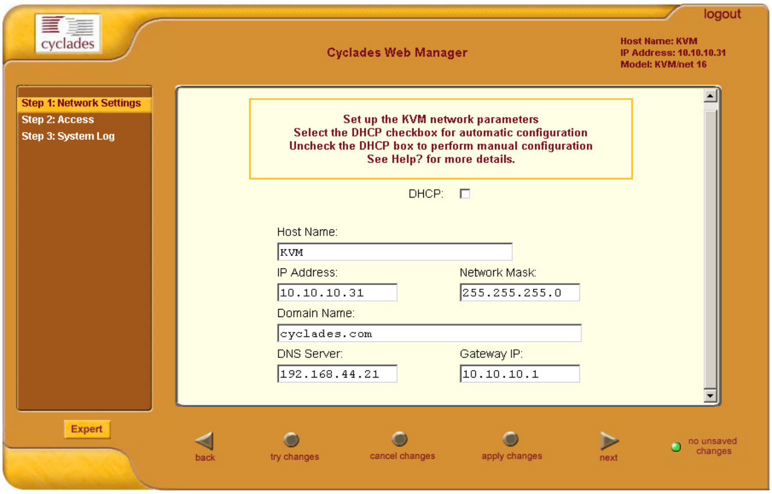
Host Name: KVM
IP Address: 10.10.10.31
Model: KVM/net 16

Set up the KVM network parameters
Select the DHCP checkbox for automatic configuration
Uncheck the DHCP box to perform manual configuration
See Help? for more details.

DHCP: ☑

2. If DHCP is your preferred setting, proceed to **Step 2: Access**; if not, click on the checkbox to deselect DHCP and enter your network settings manually.

   The Network Settings entry fields should appear as shown:



Host Name: KVM
IP Address: 10.10.10.31
Model: KVM/net 16

Set up the KVM network parameters
Select the DHCP checkbox for automatic configuration
Uncheck the DHCP box to perform manual configuration
See Help? for more details.

DHCP: □

Host Name: KVM

IP Address: 10.10.10.31   Network Mask: 255.255.255.0

Domain Name: cyclades.com

DNS Server: 192.168.44.21   Gateway IP: 10.10.10.1

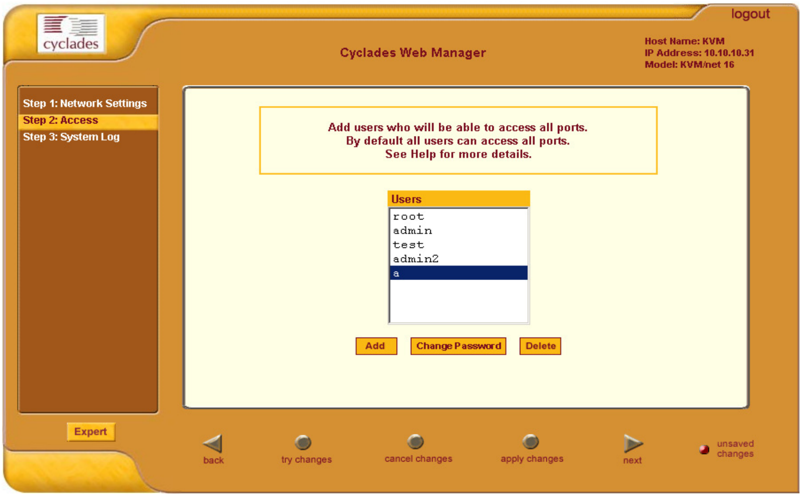
3. Type in the network information in the corresponding entry fields, and then select **Apply Changes**.
4. Select the **Next** button OR proceed to **Step 2: Access**.

Step 2: Access

The Access form allows you to add or delete users from the Users Access List. It also allows you to set or change the password for each user.

1. From the main menu of the web interface, select **Step 2: Access**.

   The system brings up the Access form:



Host Name: KVM
IP Address: 10.10.10.31
Model: KVM/net 16

Add users who will be able to access all ports.
By default all users can access all ports.
See Help for more details.

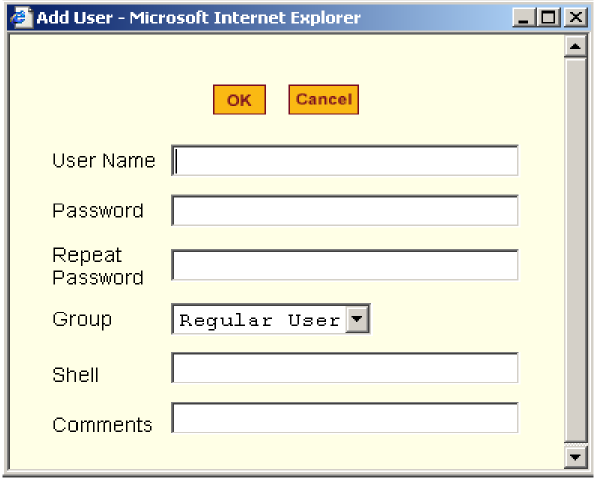
Users
root
admin
test
admin2
a

The Access form is composed of a Users list box and three buttons: **Add**, **Change Password**, and **Delete**.

To add a User

1. From the Access form, select the **Add** button.

   The system invokes the Add User dialog box:



2. Type in the necessary information as follows:

Field Name	*Definition*
User Name	Name of the user to be added to the Access List.
Password	The user password required to access the port.
Repeat Password	As indicated.
Group	Select whether the user is a **Regular User** or an **Admin**.
Shell	The default shell the user will get when they ssh or telnet into the KVM/net. Choices are: **sh** or **bash**.
Comments	Notes pertaining to the current user or setting.

3. From the dialog box, select **OK** when done.
4. From the Access form, select **Apply Changes** to save your configuration.

*To define a new user group, select the **Expert** button to switch to the Expert Mode, and then select **Configuration** (top menu) > **Users and Groups** (side menu).*

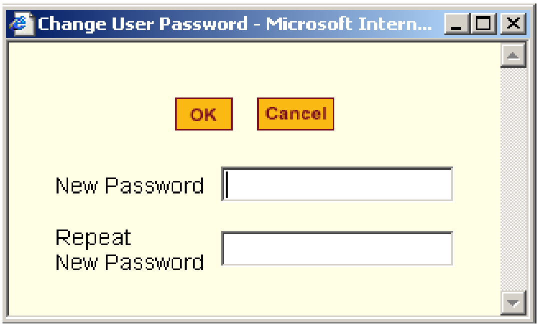
To Delete a User

1. From the users list box of the Access form, select the user that you want to delete.
2. Select the **Delete** button
3. Select the **Apply Changes** button.

To Change a User's Password

*It is recommended that you change your admin password as soon as you begin configuring the KVM/net system. If you haven't changed your password, now is the time to change it using the **Change User Password** dialog box.*

1. From the Users List box of the Access form, select the user whose password you would like to change.
2. Select the **Change Password** button.
   The system invokes the Change User Password dialog box:



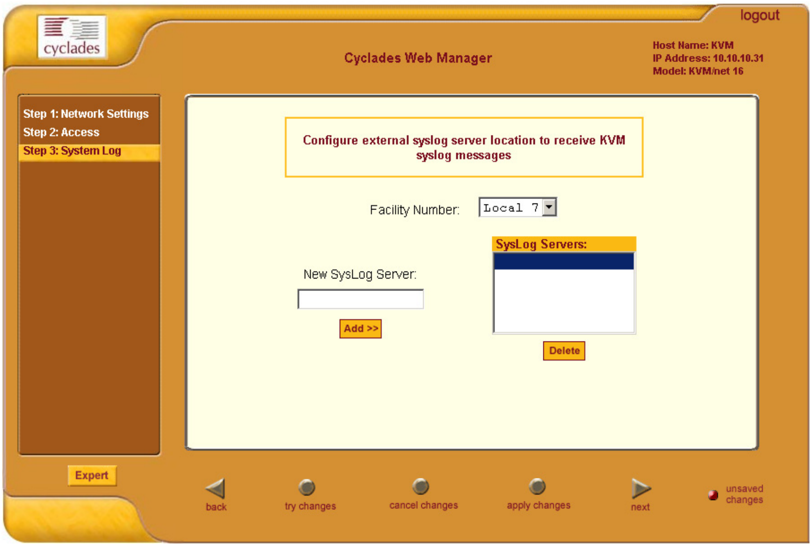
3. Enter the password in both fields and then select **OK**.
4. From the Access form, select **Apply Changes** to save your configuration.

Step 3: System Log

The System Log form is used to assign or add syslog servers to external server locations. These servers receive KVM/net syslog messages. You can also delete the servers from their locations.

1. Select Step 3: System Log from the main menu.

   The system brings up the System Log form:



Host Name: KVM
IP Address: 10.10.10.31
Model: KVM/net 16

Configure external syslog server location to receive KVM syslog messages

Facility Number: Local 7

New SysLog Server:

SysLog Servers:

To Add a Syslog Server

1. From the **Facility Number** dropdown list, select the facility number from which you want to configure your syslog servers.
2. From the New Syslog Server field, enter the IP address of the syslog server that you are adding, and then select the Add button. (Repeat this step for as many servers you need to add.)

   The new server appears in the Syslog Servers list box.
3. Select **Apply Changes** to save your configuration.

To Delete a Syslog Server

1. From the **Facility Number** dropdown list, select the facility number from which you want to configure your syslog servers.

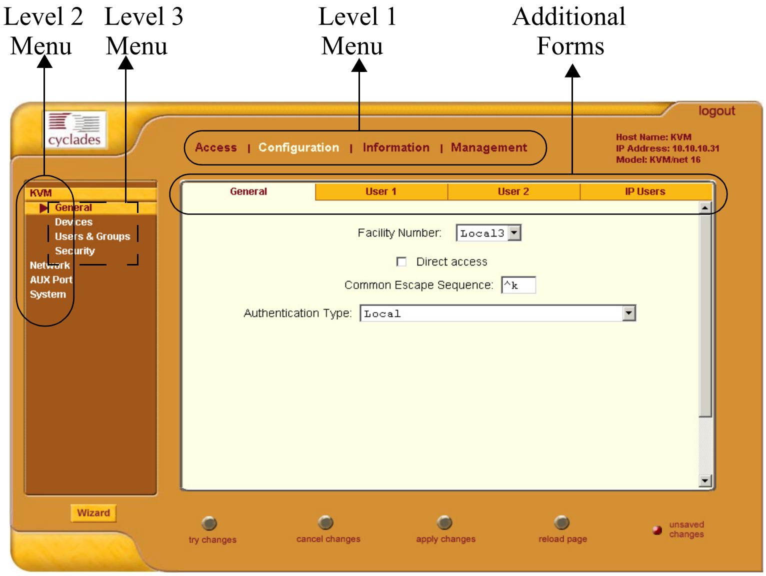
2. From the Syslog Server list box, select the syslog server that you want to delete from the current facility location, and then select **Delete**. (Repeat this step for as many servers you need to delete.)
3. Select **Apply Changes** to save your configuration.

Configuring in Expert Mode

This section presents the procedures for configuring the KVM/net web interface in Expert Mode. This mode is designed for the admin user who needs to configure the KVM/net beyond the capabilities of the basic wizard mode. A main difference between the two modes is the addition of a top menu bar in the Expert Mode to support a wider array of menu choices.

The top menu bar supercedes the left menu panel. Based on what you select from the top menu bar, the selections from the left menu panel changes accordingly.

Additionally, the left menu selection can have child windows or forms which are presented as tabbed forms within the initial form or as a second column (Level 3 menu) in the left menu panel.



Host Name: KVM
IP Address: 10.10.10.31
Model: KVM/net 16

Facility Number: Local3

☐ Direct access

Common Escape Sequence: ^k

Authentication Type: Local

Typographically, the menu path for, say, the **User 2** form would be: **Configuration** > **KVM** > **General** > **User 2**.

Table of Menu and Forms

The forms that compose the entire configuration interface in Expert Mode is as follows:

Menu Selection	*Form Name*
Access	
> Connect to Server	*This is a form by itself.*
> Power Management	**Outlets Manager** (*tab 1*)
	View IPDUs Info (*tab 2*)
	Users Manager (*tab 3*)
	Configuration (*tab 4*)
	Software Upgrade *(tab 5*)
Configuration	
> KVM	**General** (*tab 1*)
	User 1 (*tab 2*)
	User 2 (*tab 3*)
	IP Users (*tab 4*)
	Devices
	Users & Groups
	Security
> Network	**Host Settings**
	Syslog
	Services
	IP Filtering
	VPN
	SNMP
	Host Table
	Static Routes
> AUX(iliary) **Port**	*This is a form by itself.*
> System	**Date/Time**
	Boot
Information	
> General	*This is a form by itself.*
> Port Status	*This is a form by itself.*

Menu Selection	*Form Name*
Management	
> Backup Configuration	*This is a form by itself.*
> Firmware Update	*This is a form by itself.*
> Microcode Update	*This is a form by itself.*
> Microcode Reset	*This is a form by itself.*
> Active Sessions	*This is a form by itself.*
> Reboot	*This is a form by itself.*

Most of the form fields are defined in the procedure section of each form. For a more detailed definition of the field names or terms, refer to the ***Glossary*** *of this manual.*

Access

The **Access** form is used by the regular user to select and access ports as well as to view power management (IPDU settings) information. The first selection, **Connect to Server**, is designed for the KVM/net regular user and is discussed in more detail in **Chapter 4: KVM/net Operation**.

Access

Menu Selection	*Use this form to:*
Connect to Server	Select and connect to a port.
Power Management	View and edit IPDU settings.This menu comprises five tabbed forms: Outlets Manager, View IPDUs Info, Users Manager, Configuration, and Software Upgrade.

Power Management

Power Management comprises five tabbed forms, which are designed to configure any Cyclades AlterPath Power Manager unit connected to the KVM/net switch.

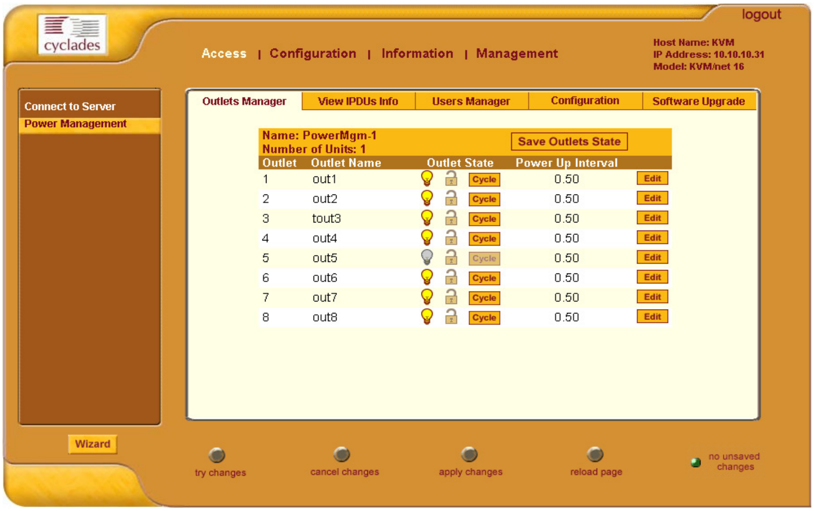
Menu Selection	*Use this form to:*
Outlets Manager	Switch on/off and lock/unlock outlets; reboot network devices.
View IPDUs Info	View IPDU information by ports and slaves. The information form provides real-time, global, current monitoring of all connected devices.
Users Manager	Add or delete users assigned to specific outlets.
Configuration	Enable over power protection, syslog and alarm notification from any specified port. The form allows you to set a current alarm threshold that once exceeded will have the KVM/net sound an alarm or send a notification message.
Software Upgrade	Upgrade the AlterPath Power Manager software.

Power Management > Outlets Manager

The **Outlets Manager** form allows you to check the status of all IPDUs connected to the Console Server, including their outlets. Any user who has Administration privileges can turn on, turn off, cycle (*i.e.*, to automatically switch off and on), lock and unlock the outlets.

1. From the top menu, select **Access**; from the left menu, select **Power Management**.

   The system invokes the **Outlets Manager** tabbed form:



Host Name: KVM
IP Address: 10.10.10.31
Model: KVM/net 16

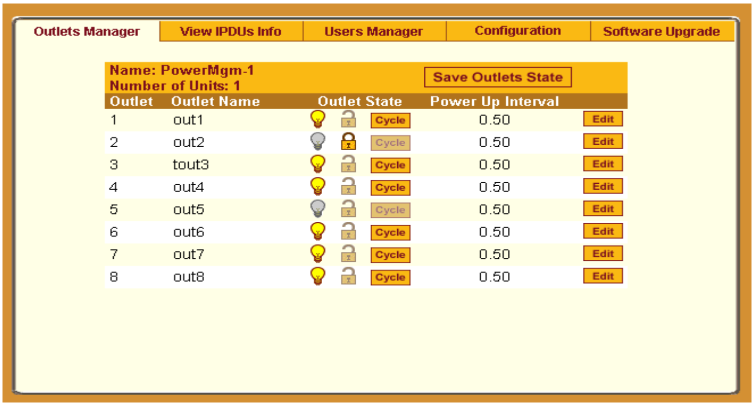
Name: PowerMgm-1
Number of Units: 1

Outlet	Outlet Name	Outlet State	Power Up Interval	
1	out1	● 🔓 Cycle	0.50	Edit
2	out2	● 🔓 Cycle	0.50	Edit
3	tout3	● 🔓 Cycle	0.50	Edit
4	out4	● 🔓 Cycle	0.50	Edit
5	out5	○ 🔓 Cycle	0.50	Edit
6	out6	● 🔓 Cycle	0.50	Edit
7	out7	● 🔓 Cycle	0.50	Edit
8	out8	● 🔓 Cycle	0.50	Edit

In the example above, the yellow bulbs (*i.e*, this is the actual color online when the switch is ON) and the opened padlock indicate that the outlets are switched on and unlocked.

2. To switch on/off an outlet, click on the light bulb; to lock/unlock an outlet, click on the padlock.

   In the sample form below, outlet 1 has been locked; outlet 2 has been switched off and locked.



Name: PowerMgm-1
Number of Units: 1

Outlet	Outlet Name	Outlet State			Power Up Interval	
1	out1	💡	🔓	Cycle	0.50	Edit
2	out2	○	🔒	Cycle	0.50	Edit
3	tout3	💡	🔓	Cycle	0.50	Edit
4	out4	💡	🔓	Cycle	0.50	Edit
5	out5	○	🔓	Cycle	0.50	Edit
6	out6	💡	🔓	Cycle	0.50	Edit
7	out7	💡	🔓	Cycle	0.50	Edit
8	out8	💡	🔓	Cycle	0.50	Edit

3. To save your changes, click on the **Save Outlets State** button located in the form.
4. Click on the **Apply Changes** button located at the bottom of the configuration window.

Power Management > View IPDUs Info

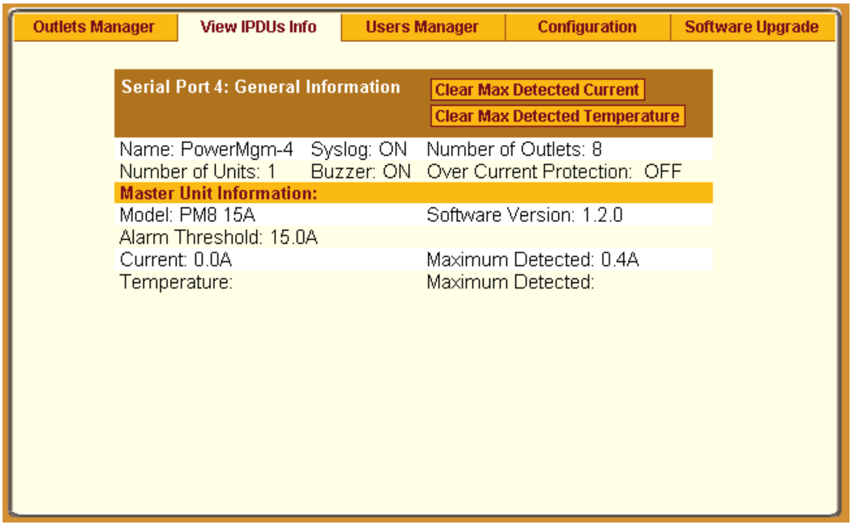
The IPDU Info form allows you to view all IPDU information (*e.g.*, number of outlets of each unit, current, temperature, alarm threshold levels, firmware, etc.) by serial port.

The form stores historical values of the maximum current and the maximum temperature.

To view the IPDU information, perform the following steps:

1. From the top menu, select **Access**; from the left menu panel, select **Power Management**; from the form tabs, select **View IPDUs Info**.

   The system brings up the **IPDUs Info** form:



Serial Port 4: General Information

Name: PowerMgm-4	Syslog: ON	Number of Outlets: 8
Number of Units: 1	Buzzer: ON	Over Current Protection: OFF
Master Unit Information:		
Model: PM8 15A		Software Version: 1.2.0
Alarm Threshold: 15.0A		
Current: 0.0A		Maximum Detected: 0.4A
Temperature:		Maximum Detected:

2. To delete the stored values for the maximum detected current, select the **Clear Max Detected Current** button.
3. To delete the stored values for the maximum detected temperature, select the **Clear Max Detected Temperature** button.

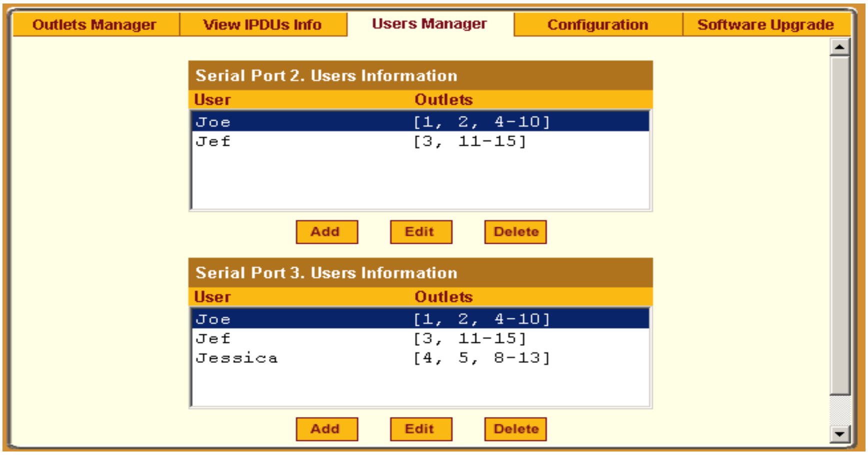
Power Management > Users Manager

The Users Management form of Power Management allows you to assign users to selected outlets for each serial port, and vice versa.

To add a user or edit an assigned user:

1. From the top menu bar, select **Access**; from the left menu panel, select **Power Management**; from the tabs, select **Users Manager**.

   The system brings up the **Users Manager** form:



Serial Port 2. Users Information

User	Outlets
Joe	[1, 2, 4-10]
Jef	[3, 11-15]

Serial Port 3. Users Information

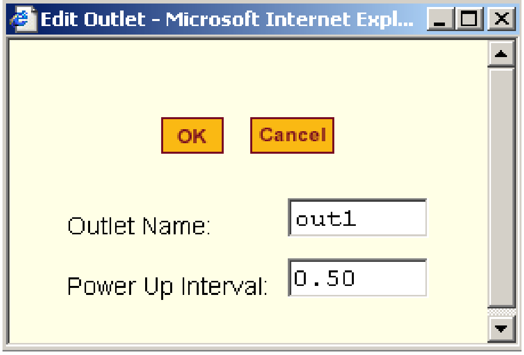
User	Outlets
Joe	[1, 2, 4-10]
Jef	[3, 11-15]
Jessica	[4, 5, 8-13]

2. To edit an assigned user, select the user you wish to edit from the Serial Port view table and then select the **Edit** button that corresponds to the table.

   - OR -

   To add or assign a new user select the **Add** button from the appropriate Serial Port view table.

The system brings up the **Edit Outlet** dialog box:



Outlet Name: out1

Power Up Interval: 0.50

3. From the Add/Edit User dialog box, modify or enter in the corresponding fields the user and the outlets to which the user is assigned, and then select the **OK** button.

*In the **Outlets** field, use the comma to separate each outlet; use the hyphen to indicate a range of outlets (e.g., 1, 3, 6, 9-12).*

*Selecting **Edit** will not allow you to edit or delete the user, only the outlet assignments for that user.*

4. Verify your entry by checking the appropriate Serial Port table from the Users Manager form.
5. Select the **Apply Changes** button located at the bottom of the Access Power Management form.

To delete an assigned user

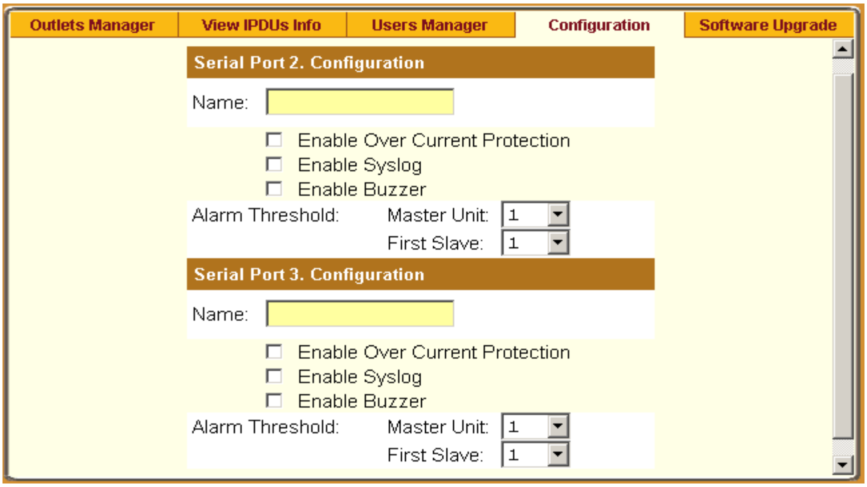
1. Select the user you wish to delete from the appropriate Serial Port view table.
2. Based on the Serial Port view table that you are working on, select the corresponding **Delete** button.

Power Management > Configuration

To configure IPDUs to generate alarms or syslog files, perform the following steps:

1. From the top menu, select **Access**; from the left menu panel, select **Power Management**; from the default Outlets Manager form select the **Configuration** tab.

   The system brings up the Configuration form:



Serial Port 2. Configuration

Name:

□ Enable Over Current Protection
□ Enable Syslog
□ Enable Buzzer

Alarm Threshold: Master Unit: 1
First Slave: 1

Serial Port 3. Configuration

Name:

□ Enable Over Current Protection
□ Enable Syslog
□ Enable Buzzer

Alarm Threshold: Master Unit: 1
First Slave: 1

2. From the Configuration form, select the Serial Port you wish to configure and then click on the appropriate radio buttons to enable/disable Over Current Protection, Syslog, and Buzzer.
3. If enabling the buzzer or alarm notification, provide the Alarm Threshold (1-100 amps) for that master or slave unit.
4. Click on the **Apply Changes** button at the bottom of the form.

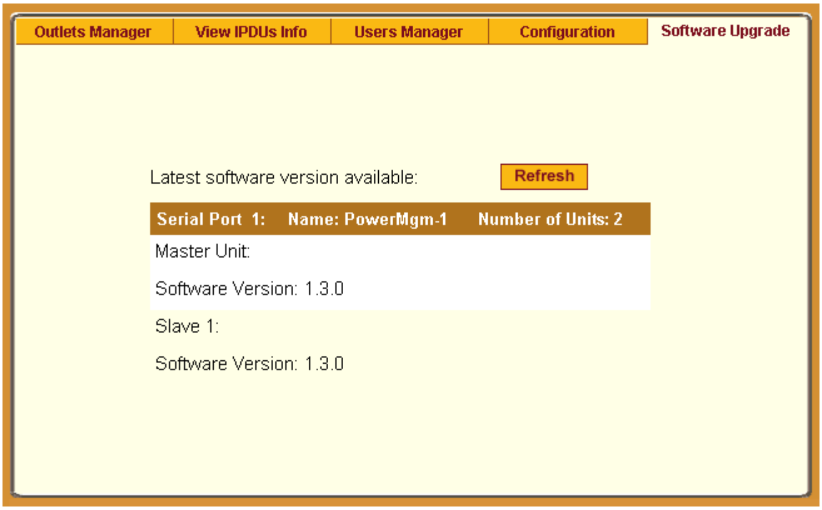
Power Management > Software Upgrade

The **Software Upgrade** form of Power Management allows you to upgrade the Power Management software for a selected serial port. The first line of the form shows the **latest software version available**. The presence of an **Upgrade** button indicates that a new software version for that master or slave port is available.

To upgrade the software for a selected port, perform the following steps:

1. From the top menu, select **Access**; from the left menu, select **Power Management**; from the tabs, select **Software Upgrade**.

   The system brings up the **Software Upgrade** form:



Latest software version available:

Serial Port 1: Name: PowerMgm-1 Number of Units: 2

Master Unit:

Software Version: 1.3.0

Slave 1:

Software Version: 1.3.0

2. Select the **Refresh** button to ensure that all software information on the form is up-to-date.
3. From the Software Version list, select the software you wish to update, and then select the **Update** button to the right of the listed version.

   *The above form example does not have an **Update** button associated with any of the software versions listed, which means that they are up-to-date and there is no need to update them.*
4. Select the **Apply Changes** button at the bottom of the configuration window to save your configuration.

Configuration

Configuration, the second primary menu selection, is composed of four menu selections with the following child menus and forms:

- **KVM -** General (composed of four tabbed forms), Devices, Users & Groups, and Security)
- **Network -** Host Settings, Syslog, Services, IP Filtering, VPN, SNMP, and Host Table.
- **AUX Port -** no other forms associated.
- **System -** Date/Time and Boot

KVM

Composed of four tabbed forms, the first selection allows you to configure the following KVM/net settings:

Form Name	*Use this form to:*
General	Define the Facility Number (i.e., the location of the managed server/s), IP settings, and authentication type.
User 1	Configure the first user's console and keyboard settings: Idle Timeout, Screen Saver Timeout, and various key commands (*a.k.a.* escape sequences).
User 2	Configure the second user's console and keyboard settings: Idle Timeout, Screen Saver Timeout, and various key commands (*a.k.a.* escape sequences).
IP Users	Configure the web user's console and keyboard settings: Idle Timeout, Screen Saver Timeout, and various key commands (*a.k.a.* escape sequences).

Default Key Sequences

A main component of the KVM/net settings is defining the key sequences for users when using the AlterPath Viewer. A *key sequence* (also known as *escape sequence*) is a sequence of special characters used to send a command to a device or program, in this case the KVM/net application. Typically, an escape sequence begins with an escape character (hence, the term), but this is not always the case.

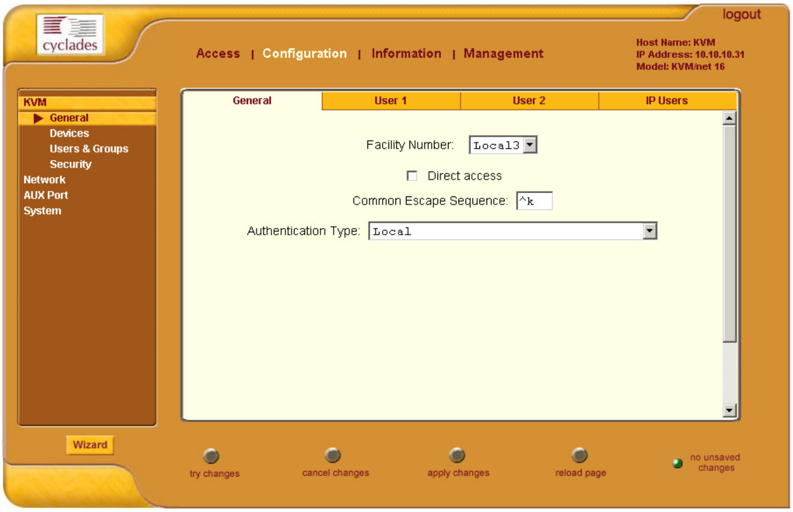
In KVM/net, the default key sequence (Ctrl-K, Q) for getting out of a particular window while connected to a port is also called *escape sequence*.

Aside from the navigation keys listed above, you can use the following key sequences to perform a specific action:

Key Sequence	*Action*
Ctrl-K, and then Q	Quit command - closes the session to a port and takes you back to the KVM/net Main Menu.
Ctrl-K, and then P	Port command - initiates a power control session.
SCROLL LOCK twice, and then L	RP Switch to Local command - switches the AlterPath KVM RP video display to the local computer.
SCROLL LOCK twice, and then R	RP Switch to Remote command - switches the AlterPath KVM RP video display to the remote computer.
Ctrl-K, and then C	KVM/net Switch command - switches from the currently connected server to your next authorized server.
Ctrl-K, and then V	Video command - controls screen brightness and contrast.
Ctrl-K, and then S	Keyboard and Mouse Synchronization command - resets the keyboard and mouse synchronization if either one becomes unavailable after adding a new server to the KVM/net.

1. To configure the KVM/net Settings, from the top menu, select **Configuration**; form the left menu, select **KVM**.

   The system brings up the first of four forms under KVM: **General** form:



Host Name: KVM
IP Address: 10.10.10.31
Model: KVM/net 16

Facility Number: Local3

□ Direct access

Common Escape Sequence: ^k

Authentication Type: Local

2. From the **General** form, complete the data entry fields as follows:

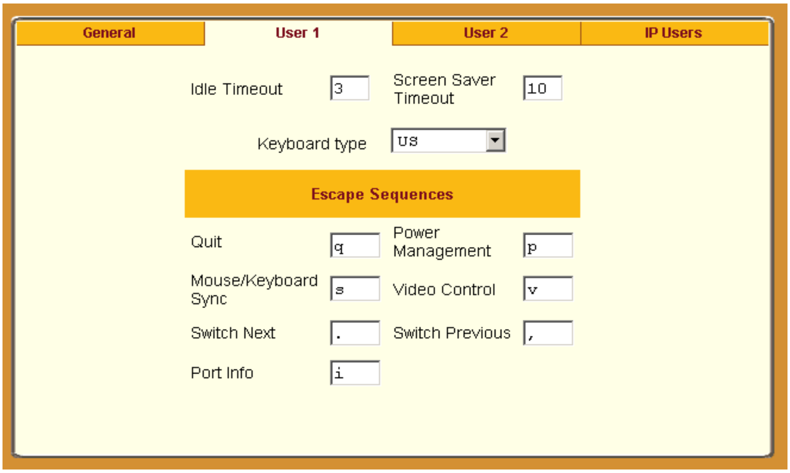
Field Name	*Definition*
Facility Number	Define the Facility Number (i.e., the location of the managed server/s).
Direct Access	Select this check box to enable direct access to a port as the user logs in from the Login screen.
Common Escape Sequence	The recommended key combinations are the control key followed by a letter key (*e.g.*, Ctrl + Q).
Authentication Type	Choice of authentication services are: None, Local, Radius, TacacsPlus, Ldap, Kerberos, and NTLM.

3. Click on Apply Changes to save your configuration.
4. If you need to configure another facility, select a new Facility Number and then repeat steps 2 and 3.

   - OR -

   Proceed to the next form by clicking on the **User 1** tab.

The system brings up the **User 1** form:



Idle Timeout	3	Screen Saver Timeout	10
Keyboard type	us		

Escape Sequences

Quit	q	Power Management	p
Mouse/Keyboard Sync	s	Video Control	v
Switch Next	.	Switch Previous	,
Port Info	i		

The **User 1** form is used to configure the first user’s console and keyboard settings.

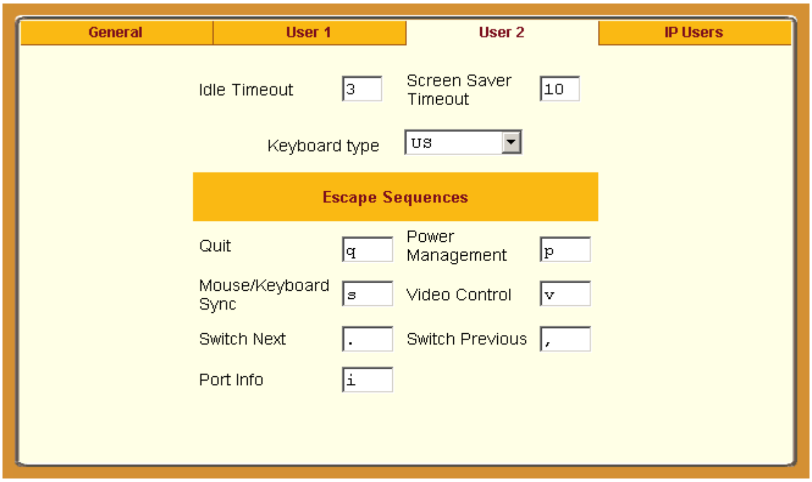
5. From the **User 1** form, complete the data entry fields as follows:

Field Name	*Definition*
Idle Timeout	The time (in minutes) it takes the system to timeout after it remains idle.
Screen Save Timeout	The time (in minutes) it takes for the screen saver to activate after the system remains idle.
Keyboard Type	From the drop-down list, select the keyboard type assigned to User 1.
Quit	Key sequence for quit.
Power Management	Key sequence for Power Management.
Mouse/Keyboard Sync	Key sequence for M/K synchronization.
Video Control	Key sequence for video control.
Switch Next	Key sequence for switching to the next screen.
Switch Previous	Key sequence for switching to the previous screen.
Port Info	Key sequence for invoking the Port Information screen.

6. Click on **Apply Changes** to save your configuration.

7. Proceed to the next form by clicking the **User 2** tab.

   The system brings up the **User 2** form:



Idle Timeout	3	Screen Saver Timeout	10
Keyboard type	US		

Escape Sequences

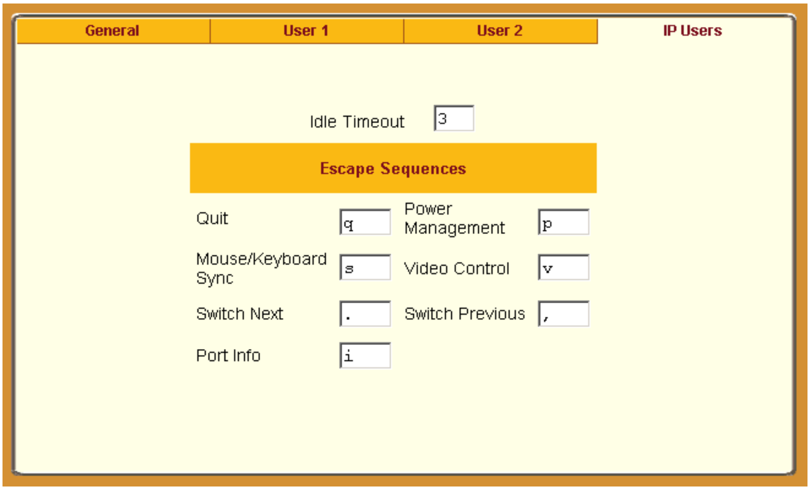
Quit	q	Power Management	p
Mouse/Keyboard Sync	s	Video Control	v
Switch Next	.	Switch Previous	,
Port Info	i		

The **User 2** form is used to configure the second user's console and keyboard settings.

8. Complete the data entry fields for User 2, and then click on the **Apply Changes** button to save your configuration.

   For a definition of the fields, see the field definition table from step 5.

9. Proceed to the next form by clicking on the **IP Users** tab.
   The system brings up the **IP Users** form:



Idle Timeout 3

Escape Sequences

Quit	q	Power Management	p
Mouse/Keyboard Sync	s	Video Control	v
Switch Next	.	Switch Previous	,
Port Info	i		

The **IP Users** form is used to configure the web user's console and keyboard settings.

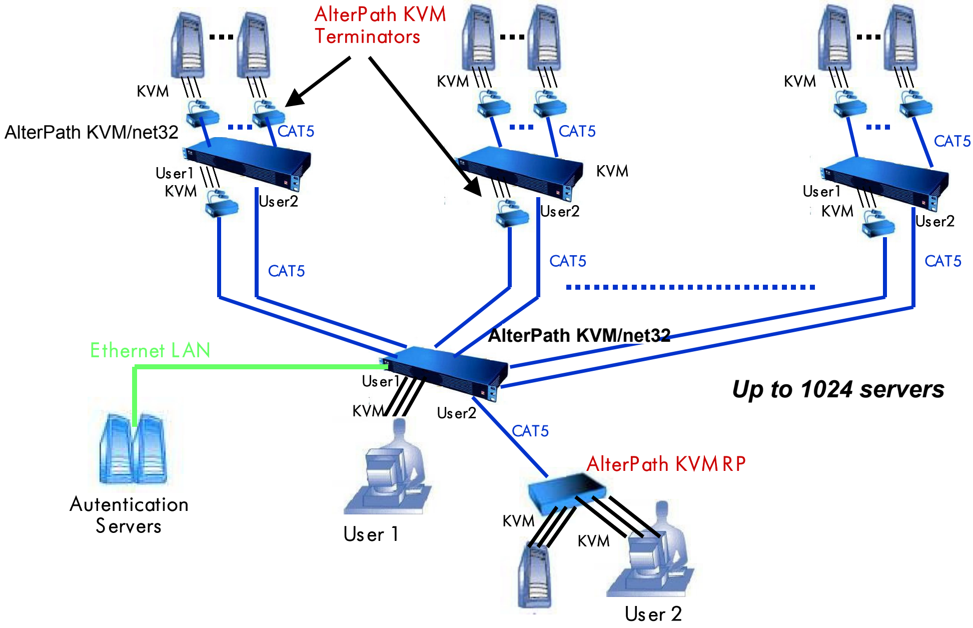
10. Complete the data entry fields for Web User, and then click on the **Apply Changes** button to save your configuration.

Devices

The **Devices** form allows you to configure one or more slave KVM units to a master KVM/net unit, a process also known as *cascading* or *daisy-chaining*.

If you already understand cascading, skip this introduction and proceed to the procedural sections.

Cascading refers to the multiple connections of slave devices to a KVM/net master for as many allowable tiers or hierarchies. For example, a 2-tier, cascaded configuration can have KVM slaves connected to a KVM/net master. The diagram below shows a basic cascaded configuration of a KVM/net 32 master with all KVM components.

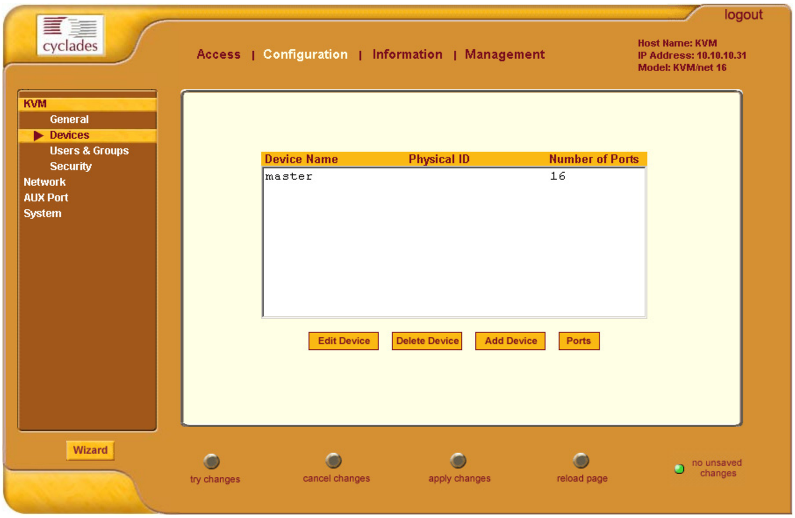


Using the KVM/net 32, 32 master KVM/net units or switches can be cascaded for a total of up to 32 units (regardless of how many times they are cascaded). A 2-user configuration can control up to 512 servers; a single user, up to 1024 servers (*i.e.*, from a single keyboard-monitor-mouse console, either locally or remotely through the ethernet LAN).

To add a KVM/net slave to be cascaded to a master KVM/net:

1. From the top menu, select **Configuration**; form the side menu, select **Devices**.

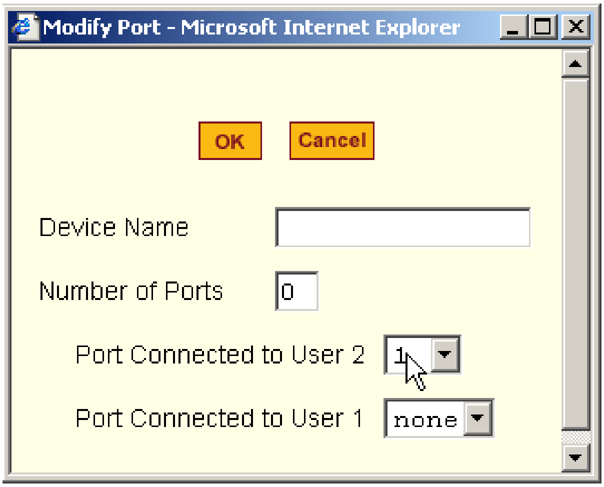
   The system brings up the **Devices** configuration form:



Device Name	Physical ID	Number of Ports
master		16

2. From the **Devices** configuration form, select the **Add** button.

   The system brings up the **Modify Port** dialog box:



Device Name

Number of Ports 0

Port Connected to User 2 1

Port Connected to User 1 none

3. Complete the dialog box as follows:

Field Name	*Definition*
Device Name	Name of the slave device or KVM switch.
Number of Ports	Number of ports contained in the device to be cascaded.
Port Connected to User 2	The KVM slave port to be connected to the User 2 port of the master KVM/net.
Port Connected to User 1	The KVM slave port to be connected to the User 1 port of the master KVM/net.

4. Select the **OK** button when done.
5. From the configuration window, select **Apply Changes** to save your configuration.

<u>To edit a device configuration:</u>

1. From the top menu, select **Configuration**; form the side menu, select **Devices**.

   The system brings up the **Devices** configuration form.
2. From the Device list box, select the line item you wish to edit, and then select the **Edit** button.

   The system brings up the Modify Port dialog box which is similar to the dialog box used for adding a port.
3. From the dialog box, modify the configuration as necessary (see field definition table from the preceding procedure), and then select the **OK** button.
4. From the configuration window, select **Apply Changes** to save your configuration.

<u>To delete a device configuration:</u>

1. From the top menu, select **Configuration**; form the side menu, select **Devices**.

   The system brings up the Cascading configuration form.
2. From the Device list box, select the line item you wish to delete, and then select the **Delete** button.

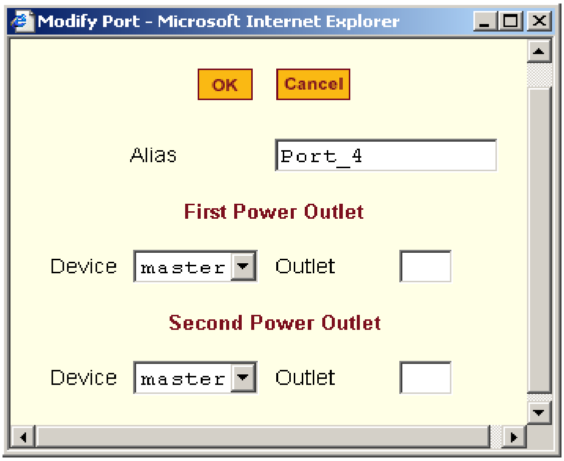
   The system deletes the selected line item from the Device list box.
3. From the configuration window, select **Apply Changes** to save your configuration.

To Configure Ports

The Ports dialog box is used to modify the power outlet assignments for each port connected to the KVM/net, as well as to enable/disable the ports.

1. From the Devices form (**Configuration** > **KVM** > **Devices**), select the Device that contains the port(s) to be configured.

   The system brings up the Modify Port dialog box:



Alias Port_4

First Power Outlet

Device master Outlet

Second Power Outlet

Device master Outlet

2. Enter the Device and Outlet information, as necessary, and then select the **OK** button.
3. Select the **Apply Changes** button to save your configuration.

To Enable or Disable a Port

1. From the **Devices** configuration form (**Configuration** > **KVM** > **Devices**), select the device that contains the port(s) you wish to enable or disable.
2. From the resulting dialog box, select the ports to be enabled/disabled, and then select the **Enable** or **Disable** button.
3. Verify your configuration change by checking the port status from the Ports list box.
4. Select the **Apply Changes** button to save your configuration.

Users & Groups

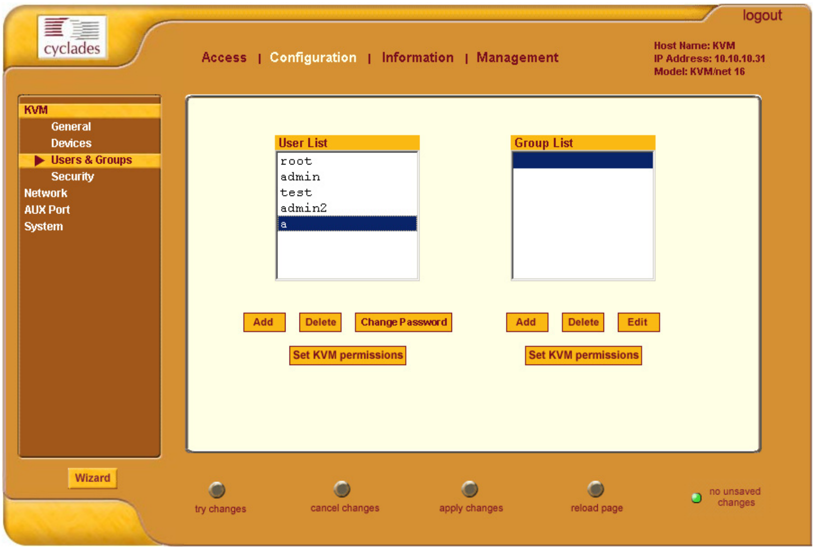
The **Users & Groups** configuration form allows you to:

- Set specific KVM/net permissions (*i.e.*, by individual port) for each user.
- Assign or change user passwords.
- Add or delete users from the User Access List.
- Set specific KVM/net permissions by group.
- Add or delete user groups from the Group Access List.

<u>To set KVM/net permissions for a user or a group:</u>

1. From the top menu, select **Configuration**; from the side menu, select **KVM** > **Users & Groups**.

   The system invokes the **Users & Groups** configuration form:

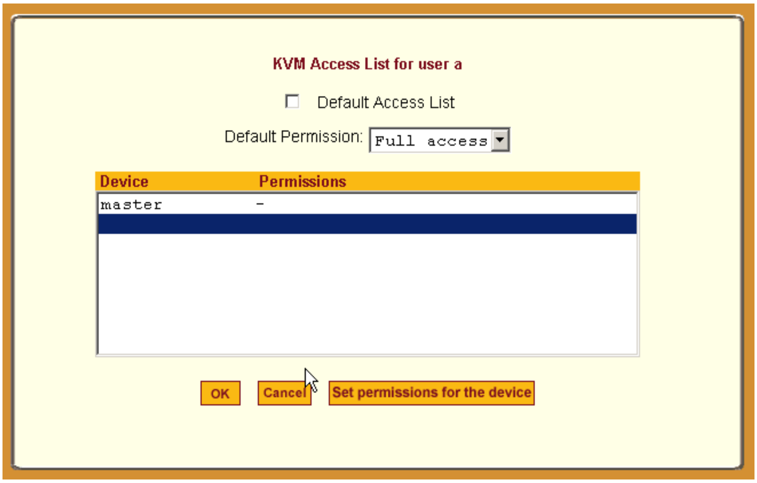


2. From the **User List** box, select the user to be configured for KVM/net permissions.

   - OR -

   From the **Group List** box, select the group to be configured for KVM/net permissions.

3. Select the corresponding **Set KVM Permissions** button.
   The system invokes the Set KVM Permissions form:



KVM Access List for user a

□ Default Access List

Default Permission: Full access

Device	Permissions
master	-

4. Complete the form as follows:

Field Name	*Definition*
Default Access List	Select this check box if you want to include the current user to the default Access List.
Default Permission	The default permission for the current user.
[Device view list]	List of devices and type of permission for each device.
Set Permissions for the Device	Button to invoke a dialog box to set or reset the permission for a selected device (from the Device view list).

5. Select **OK** when done.
6. Select **Apply Changes** at the bottom of the configuration window.

To delete a user/group from the Access List:

1. Go to **Configuration** > **KVM** > **Users & Groups**.
2. To delete a user, select the user to be deleted from the **User List** box

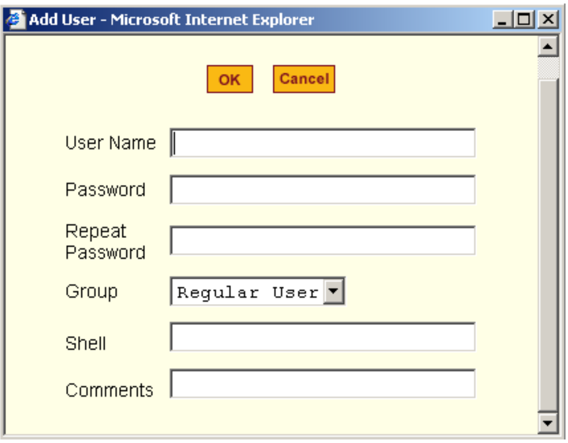
   - OR -

   To delete a group, select the group name to be deleted from the **Group List** box.
3. Select the corresponding **Delete** button.
4. Verify your deletion by checking the list box.
5. Select **Apply Changes** to save your configuration change.

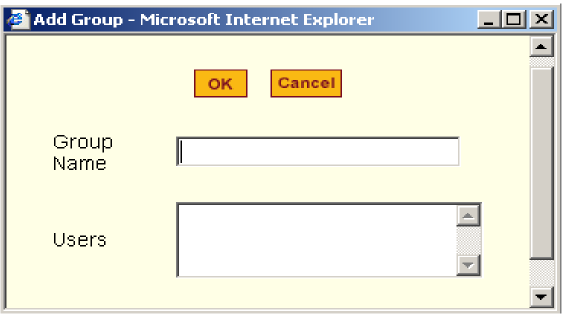
To add a user/group to the Access list (to access KVM/net ports):

1. Go to **Configuration** > **KVM** > **Users & Groups**.
2. To add a user or a group to the Access list, select the appropriate **Add** button.

   If you selected the **Add** button for the User List, the Add User dialog box appears as follows:



If you selected the **Add** button for the Group List, the Add Group dialog box appears as follows:



3. Complete the fields, as necessary, and then select **OK**.
4. From the configuration window, select **Apply Changes** to save your configuration.

To change a user's password

1. Go to **Configuration** > **KVM** > **Users & Groups**.
2. From the **User List** box, select the user whose password you would like to change, and then select the **Change Password** button.

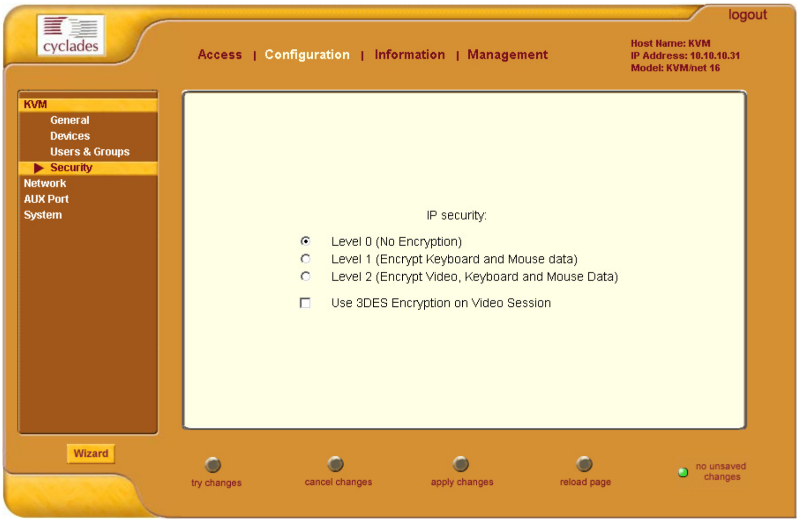
   The system brings up the Change User Password.
3. From the dialog box, type in the new password twice, and then select the **OK** button.
4. From the configuration window, select the **Apply Changes** button to save your configuration.

Security

The Security form allows you to configure your IP security.

1. From the top menu, select **Configuration**; from the side menu, select **KVM** > **Security**.

   The system brings up the Security form:



IP security:

● Level 0 (No Encryption)
○ Level 1 (Encrypt Keyboard and Mouse data)
○ Level 2 (Encrypt Video, Keyboard and Mouse Data)

□ Use 3DES Encryption on Video Session

2. Check the appropriate radio buttons.

Based on the Authentication Type that you select, the system will prompt you for additional information. For example, if you select ***Radius*** *as your Authentication service, then the system will prompt you for the addresses of the authentication servers and accounting servers, the secret, the timeout and retries.*

3. Select the **Apply Changes** button to complete the procedure.

Network

Network configuration (which is the second of four primary options that belong to the top **Configuration** menu) comprises eight forms:

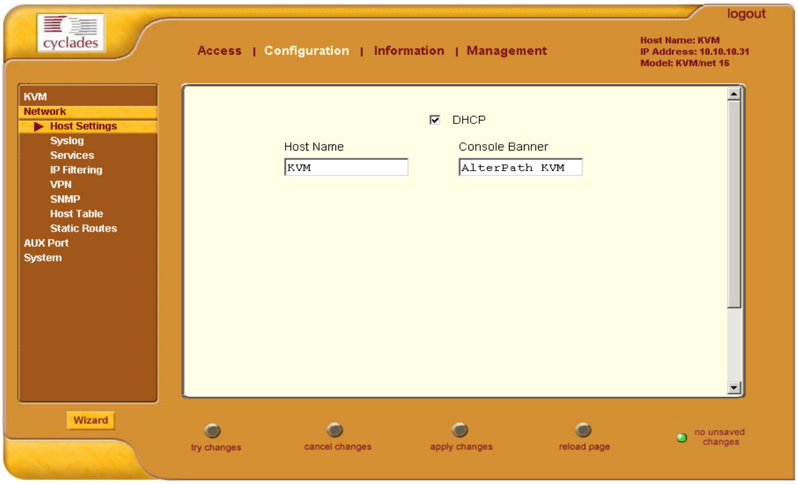
Form	*Use this form to:*
Host Settings	Configure host connections, including: Ethernet Port connections, DNS Service, and Name Service Access.
Syslog	Define the Syslog Servers to enable system logging.
Services	Define or activate the method of access (*i.e.*, Telnet, SSH, SNMP, Client, or NTP).
IP Filtering	Configure the selective filtering of packets that may potentially crack your network system or generate unnecessary traffic.
VPN	Configure IPsec tunnels to establish a secure connection between KVM/net and a security gateway machine.
SNMP	Configure the SNMP server to manage complex networks.
Host Table	View hosts list; create, edit, and delete hosts.
Static Routes	View, create and delete routes from the table.

Network > Host Settings

The Host Settings form allows you to configure the network settings for the KVM/net.

1. From the top menu, select **Network**; from the side menu, select **Host Settings**.

   The system brings up the **Host Settings** form:



Host Name: KVM
IP Address: 10.10.10.31
Model: KVM/net 16

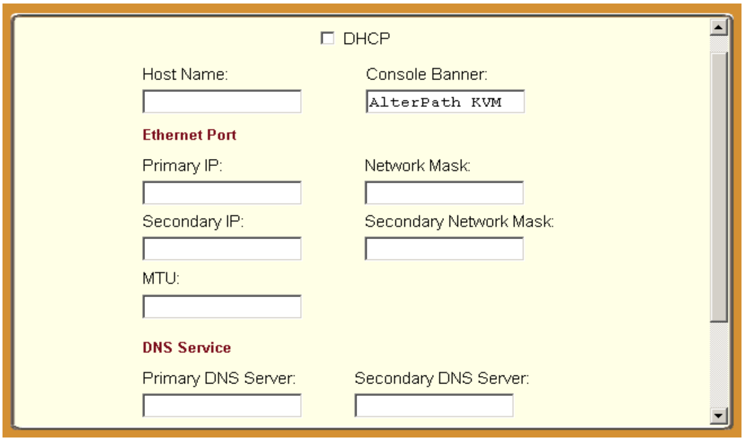
☑ DHCP

Host Name: KVM

Console Banner: AlterPath KVM

2. By default, the DHCP field is check marked. If you wish to disable DHCP and enter the host settings manually, click the checkbox to remove the check mark.

   The system should add the following fields to your form:



☐ DHCP

Host Name:

Console Banner: AlterPath KVM

Ethernet Port

Primary IP:

Network Mask:

Secondary IP:

Secondary Network Mask:

MTU:

DNS Service

Primary DNS Server:

Secondary DNS Server:

3. From the Host Settings form, complete or edit the following fields, as necessary:

Field Name	*Definition*
DHCP	This default configuration is used if you are using DHCP for your network settings.
Host Name	The fully qualified domain name identifying the specific host computer within the Internet.
Console Banner	A text string designed to appear on the console upon logging into and exiting from a port as a way to verify or identify the particular port connection.
Ethernet Port	
Primary IP	The 32-bit numeric IP address of the KVM/net unit on the Internet.
Network Mask	The 32-bit number used to group IP addresses together or to indicate the range of IP addresses for this IP network/subnet/supernet.
Secondary IP	The 32-bit numeric, secondary IP address of the KVM/net unit on the Internet.
Secondary Network Mask	The network mask of the secondary IP.
MTU	Maximum Transmission Unit used by the TCP protocol.
DNS Service	
Primary DNS Server	Address of the Domain Name Server.
Secondary DNS Server	Address of the backup Domain Name Server.
Domain Name	The name that identifies the domain (e.g., domainname.com).
Gateway IP	The gateway numeric identification number.

4. Select **Apply Changes** when done to save your configuration to flash.

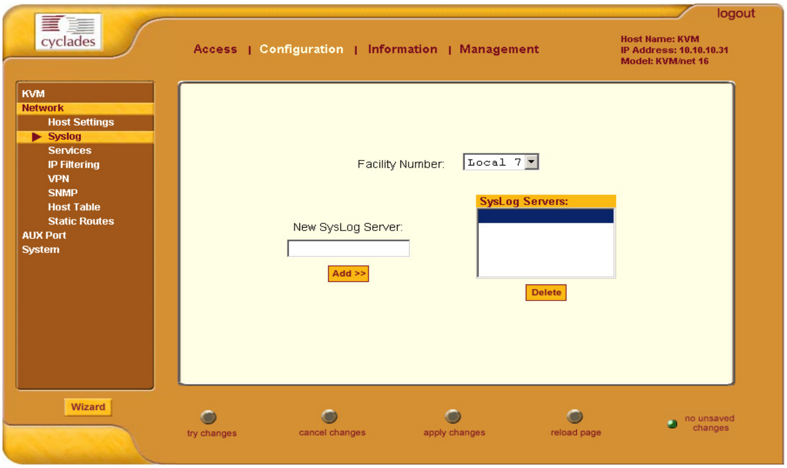
Network > Syslog

The Syslog form allows you to configure one or more syslog servers to receive KVM/net-generated syslog messages. The KVM/net generates syslog messages related to users connecting to ports, login failures and other information that can be used for audit trailing purposes. You can also use this form to delete syslog servers.

This form is the same as **Step 5: System Log** form in Wizard mode.

1. From the top menu, select **Configuration**; from the left menu, select **Network** > **Syslog**.

   The system brings up the **Syslog** form.



Facility Number: Local 7

New SysLog Server:

SysLog Servers:

2. Complete the form as follows:

Field Name	*Definition*
Facility Number	Facility number to identify the location of the Syslog Server.
New Syslog Server	Name of the Syslog Server that you wish to add.
Syslog Servers	List of all Syslog Servers connected to the KVM/net.

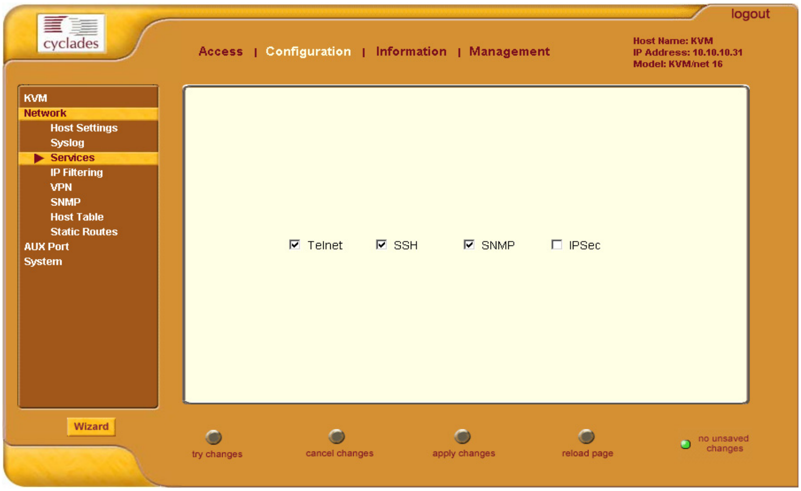
3. Select **Apply Changes** when done.

Network > Services

By selecting the appropriate box, the Services form allows you to enable or disable the daemons to use to allow different incoming connections.

1. From the top menu, select **Configuration**; from the side menu, select **Network** > **Services**.

   The system invokes the Services form.



Host Name: KVM
IP Address: 10.10.10.31
Model: KVM/net 16

☑ Telnet ☑ SSH ☑ SNMP □ IPSec

2. Select the service(s) you would to use to access devices.
3. Select **Apply Changes** when done.

Network > IP Filtering

*If you already understand how IP filtering works, skip this section and proceed to the procedure section, **IP Filtering - To Add a Chain**.*

IP filtering refers to the selective blocking of the passage of IP packets between global and local networks. The filtering is based on rules that describe the characteristics of the packet (*e.g.*, the contents of the IP header, the input/output interface, or the protocol).

This feature is used mainly in firewall applications to filter the packets that could potentially crack the network system or generate unnecessary traffic in the network.

The IP Filtering form is structured in two levels:

- Chain
- Rule

Structure of IP Filtering

IP Filtering configuration is structured on two levels:

- The IP Filtering form which contains a list of chains.
- The chains which contain the rules that control filtering.

Chain

The filter table contains a number of built-in chains and may include user-defined chains. The built-in chains are called according to the type of packet. User-defined chains are called when a rule which is matched by the packet points to the chain. Each table has a set of built-in chains classified as follows:

- INPUT - For packets coming into the box itself.
- FORWARD - For packets being routed through the box.
- OUTPUT - For locally-generated packets.

Rule

Each chain has a sequence of rules that address the following:

- How the packet should appear in order to match the rule.

  Some information about the packet is checked according to the rule, for example, the IP header, the input and output interfaces, the TCP flags and the protocol.

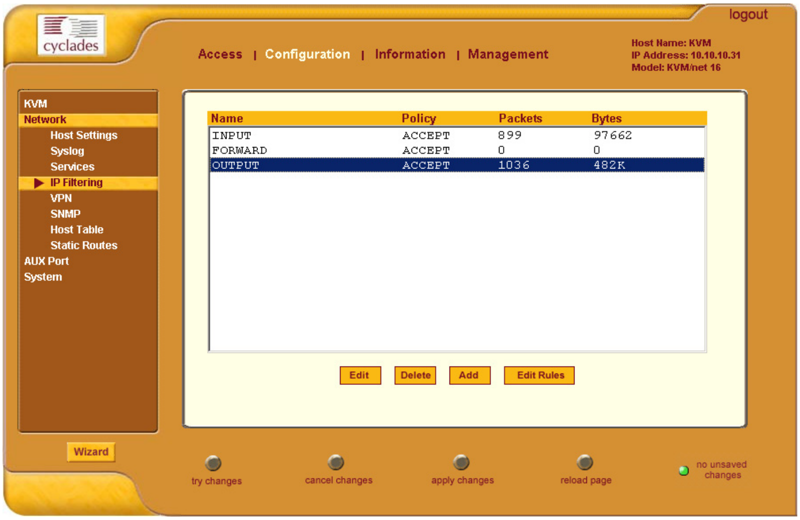
- What to do when the packet matches the rule.
  The packet can be accepted, blocked, logged or jumped to a user-defined chain.

  When a chain is analyzed, the rules of this chain are reviewed one-by-one until the packet matches one rule. If no rule is found, the default action for that chain will be taken.

IP Filtering: To add a chain:

1. From the top menu, select **Configuration**; from the left menu, select **Network** > **IP Filtering**.

   The system brings up the IP Filtering configuration form:

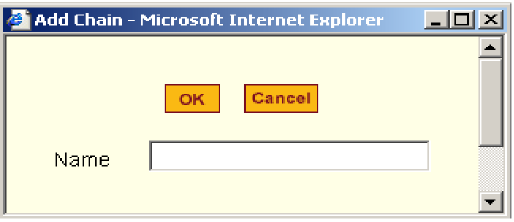


Name	Policy	Packets	Bytes
INPUT	ACCEPT	899	97662
FORWARD	ACCEPT	0	0
OUTPUT	ACCEPT	1036	482K

   Each line in the list box represents a chain. For a definition or explanation of the field columns, refer to the introductory section of this procedure or to the field definitions for the Edit Rule dialog box, next section.

2. To add a chain, select the **Add** button.

   The system brings up the **Add Chain** dialog box:

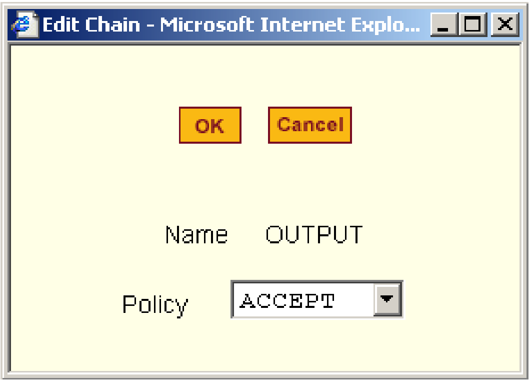


3. Enter the name of the chain that you are adding to the filter table, and then select **OK**. (Spaces are not allowed in the chain name.)
4. After entering a new chain name, click on the **Edit Rules** button to access the next dialog window to enter the rules for that chain.
5. Select **OK** to commit your changes.
6. To add rules to your new chain, see *IP Filtering: To Add a Rule* section.

IP Filtering: To edit a chain

1. From the IP Filtering form (**Configuration** > **Network** > **IP Filtering**), select the Chain you wish to edit from the Chain list box (or filter table), and then select the **Edit** button.

   The system brings up the **Edit Chain** dialog box:



Name OUTPUT

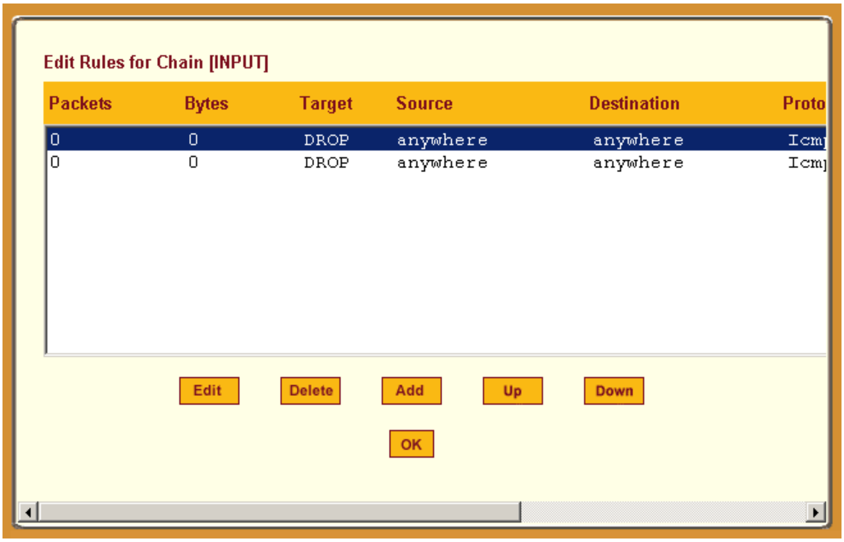
Policy ACCEPT

2. Modify the **Policy** field, as needed, and then select **OK**.
3. Verify your entry from the main form and then select **Apply Changes** to save your changes.
4. If you need to edit any rules for this chain, proceed to *IP Filtering: To Edit a Rule* section.

IP Filtering: To Edit a Rule

1. From the IP Filtering form (**Configuration** > **Network** > **IP Filtering**), select from the Chain list box (or filter table) the chain containing the rule(s) that you would like to edit, and then select the **Edit Rules** button.

   The system brings up the **Edit Rules** form:



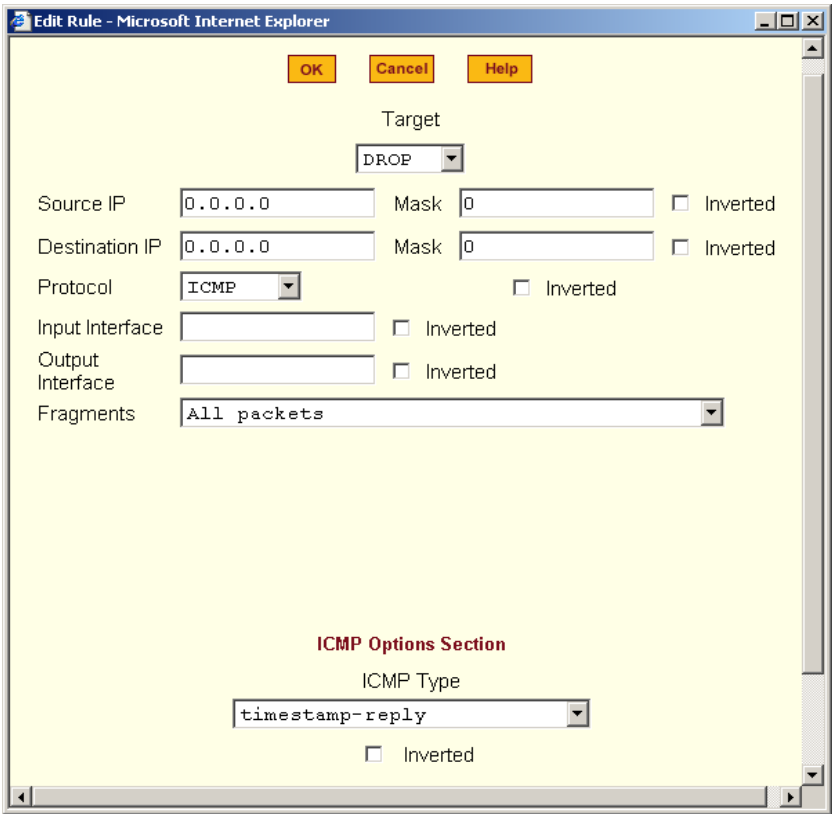
Edit Rules for Chain [INPUT]

Packets	Bytes	Target	Source	Destination	Proto
0	0	DROP	anywhere	anywhere	Icm
0	0	DROP	anywhere	anywhere	Icm

   In the example above, each line represents a rule for the INPUT chain that you selected from the Chain list box from **Step 1**. Now you must select from the above list box the rule you wish to edit.

2. From the Rules list box of the Edit Rules form, select the rule to be edited and then select the **Edit** button.

The system brings up the **Edit Rule** dialog box:



Edit Rule - Microsoft Internet Explorer

Target: DROP

Source IP: 0.0.0.0 Mask: 0 □ Inverted

Destination IP: 0.0.0.0 Mask: 0 □ Inverted

Protocol: ICMP □ Inverted

Input Interface: □ Inverted

Output Interface: □ Inverted

Fragments: All packets

ICMP Options Section

ICMP Type: timestamp-reply

□ Inverted

3. From the Edit Rules dialog box, complete the following data fields as necessary:

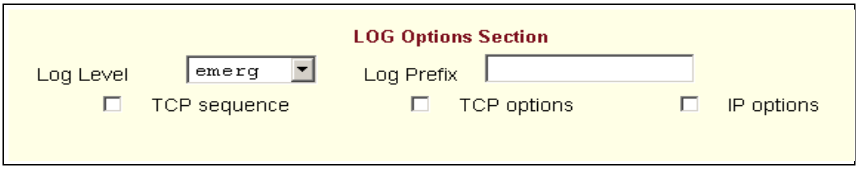
Field Name	*Definition*
Target	Indicates the action to be performed to the IP packet when it matches the rule. For example, the kernel can ACCEPT DROP, RETURN, LOG or REJECT the packet by sending a message, translating the source or the destination IP address/port or sending the packet to another user-defined chain.
Source IP	The source IP address.
Mask	Source network mask. Required when a network should be included in the rule.

Field Name	*Definition*
Inverted	Select this box to invert the target action (*i.e.*, the action assigned to the target will be performed to all source IPs/Masks except to the one just defined).
Destination IP	Destination IP address.
Mask	Destination network mask.
Inverted	Select this box to invert the target action (*i.e.*, the action assigned to the target will be performed to all Destination/Mask IPs except to the one just defined).
Protocol	The transport protocol to check. If the numeric value is available, select Numeric and type the value in the adjacent text input field; otherwise, select one of the other options.
Inverted	Select box to invert the target action (i.e., the action assigned to the target will be performed to all protocols except to the one just defined).
Input Interface	The interface where the IP packet should pass. The Input Interface option will appear only for the chains INPUT and FORWARD.
Inverted	Select box to invert the target action (*i.e.*, the action assigned to the target will be performed to all interfaces except to the one just defined).
Output Interface	The interface where the IP packet should pass. The Output interface option will appear for the chains FORWARD and OUTPUT.
Inverted	Select box to invert the target action (*i.e.*, the action assigned to the target will be performed to all interfaces except to the one just defined).
Fragments	Indicates the fragments or unfragmented packets to be checked. The IP Tables can check for: - All Packets. - 2nd, 3rd... fragmented packets. - Non-fragmented and 1st fragmented packets.
ICMP Type	This dropdown list box contains all the ICMP types that may be applied to the current rule.

Field Name	*Definition*
Inverted	This ICMP option will be applied to all rules except the currently selected rule.

Additional Fields

If you selected **Log** from the **Target** field, the following options also appear:



LOG Options Section

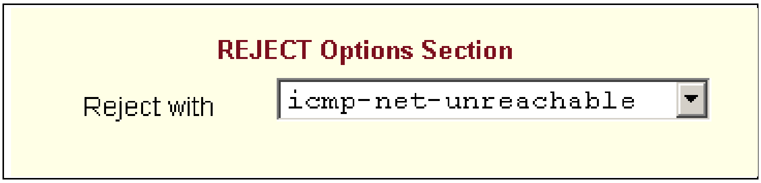
Log Level: emerg

Log Prefix:

□ TCP sequence □ TCP options □ IP options

Field Name	*Definition*
Log Level	The log level classification to be used based on the type of error message (*e.g*., alert, warning, info, debug, etc.).
Log Prefix	The prefix that will identify the log.
TCP Sequence	Check box to include TCP sequence in the log.
TCP Options	Check box to include TCP options in the log.
IP Options	Check box to include IP options in the log.

If you selected **Reject** from the **Target** field, the following field appears:



REJECT Options Section

Reject with: icmp-net-unreachable

Field Name	*Definition*
Reject with	"Reject with" means that the filter will drop the input packet and send back a reply packet according to any of the reject types listed below. Using tcp flags and appropriate reject type, the packets are matched with the REJECT target.
Choices are:	
icmp-net-unreachable	ICMP network unreachable alias.

Field Name	*Definition*
icmp-host-unreachable	ICMP host unreachable alias.
icmp-port-unreachable	ICMP port unreachable alias.
icmp-proto-unreachable	ICMP protocol unreachable alias.
icmp-net-prohibited	ICMP network prohibited alias.
icmp-host-prohibited	ICMP host prohibited alias.
echo-reply	Echo reply alias.
tcp-reset	TCP RST packet alias.

4. Click on the **OK** button when done.
5. Click on the **Apply Changes** located at the bottom of the ACS configuration window to save your configuration.

To Add a Rule

The forms and dialog boxes for adding a rule is similar to the ones used for editing a rule. Refer to *IP Filtering: To Edit a Rule* procedure section for a definition of the user input fields.

1. From the **IP Filtering** form, select the chain to which you wish to add a rule (or if you are adding a new chain, select the **Add** button and follow the procedure for adding a chain.)
2. Click on the **Edit Rule** button.

   The system brings up the **Edit Rule for Chain** dialog box.
3. From the **Edit Rule for Chain** dialog box, click on the Add button.

   The system brings up the **Add Rule** dialog box.
4. Complete the **Add Rule** dialog box. (Refer to *IP Filtering: To Edit a Rule* section for a definition of the input fields, as needed.)
5. Click on the **Apply Changes** button located at the bottom of the ACS configuration window to complete the procedure.

Network > VPN

The VPN configuration form allows you to configure one or more VPN connections to other systems or KVM/net devices.

Select one of the existing VPN connections and click the edit button or click the add button to add a new one. This launches a dialog box to prompt for the details of the connection. Complete the fields in the dialog box. The RSA keys may be entered using the Copy and Paste feature of your Browser.

If you already understand how VPN works, skip this section and proceed to the next procedure, ***To configure VPN****.*

A VPN, or Virtual Private Network lets the KVM/net and a whole network communicate securely when the only connection between them is over a third network which is untrustable. The method is to put a security gateway machine in the network and create a security tunnel between the KVM/net and the gateway. The gateway machine and the KVM/net encrypt packets entering the untrusted net and decrypt packets leaving it, creating a secure tunnel through it.

Often it may be useful to have explicitly configured IPsec tunnels between the KVM/net and a gateway of an office with a fixed IP address (in this case every machine on the office network would have a secure connection with the KVM/net), or between the KVM/net and the KVM/net administrator machine, which must, in this case, have a fixed IP address. You can add this connection descriptor to both the Console Server and the other end. This is the advantage of using left and right instead of using local remote parameters.

If you give an explicit IP address for left (and left and right are not directly connected), then you must specify leftnexthop (the router which KVM/net sends packets to in order to get them delivered to right). Similarly, you may need to specify rightnexthop (vice versa).

The Role of IPsec

IPsec is used mainly to construct a secure connection (tunnel) between two networks (ends) over a not-necessarily-secure third network. In the KVM/net, the IPsec is used to connect the KVM/net switch securely to a host or to a whole network--configurations usually referred to as *host-to-network* and *host-to-host tunnel*. Practically, this is the same thing as a VPN, but here one or both sides have a degenerated subnet (*i.e.*, only one machine).

The IPsec protocol provides encryption and authentication services at the IP level of the network protocol stack. Working at this level, IPsec can protect any traffic carried over IP, unlike other encryption which generally protects only a particular higher-level protocol (PGP for mail, SSH for login, SSL for Web work and so on). The implementation of IPsec used by the AlterPath KVM/net is FreeSWAN (www.freeswan.org).

You can use IPsec on any machine that does IP networking. Wherever required to protect traffic, you can install dedicated IPsec gateway machines. IPsec can also run on routers, firewall machines, various application servers, and end-user desktop or laptop machines.

Authentication Keys

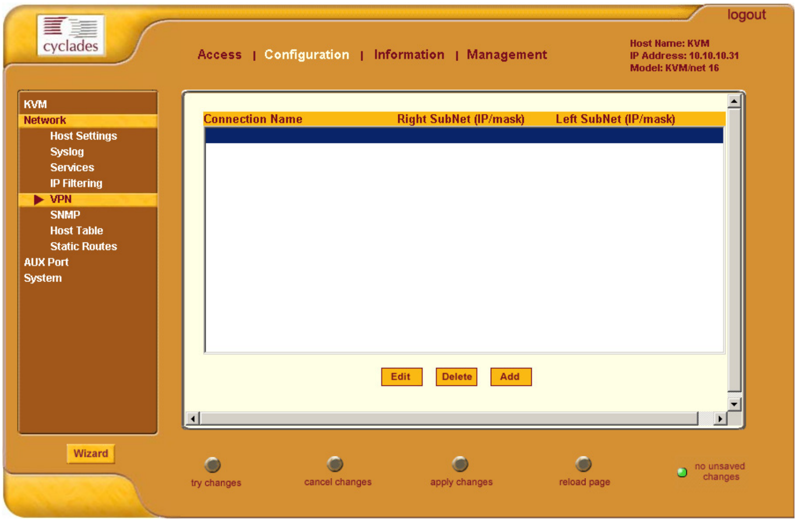
To establish a connection, the Console Server and the other end must be able to authenticate each other. For FreeS/WAN, the default is public key authentication based on the RSA algorithm.

To configure VPN

*For the VPN to function to properly, ensure that you have also enabled **IPsec** from the **Services** form.*

1. Select **Network** from the top menu bar, and then select **VPN Connections** from the left menu panel.

   The system brings up the **VPN Connections** form:



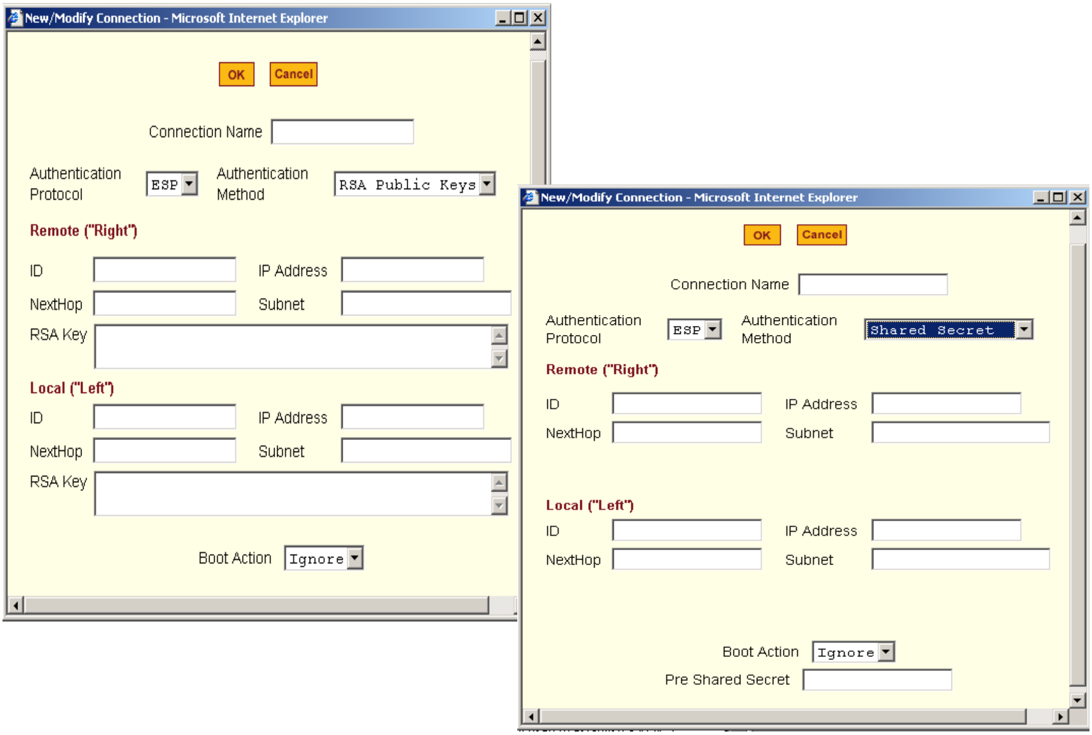
Connection Name	Right SubNet (IP/mask)	Left SubNet (IP/mask)

2. To edit a VPN connection, select the VPN connection that you wish to edit from the form, and then select the **Edit** button.

   - OR -

   To add a VPN Connection, select the **Add** button.

   The system brings up the **New/Modify Connection** dialog box:



Authentication Protocol: ESP
Authentication Method: RSA Public Keys
Boot Action: Ignore

Authentication Protocol: ESP
Authentication Method: Shared Secret
Boot Action: Ignore

If the selected **Authentication Method** is **RSA Public Keys**, the left dialog box is used. If the **Authentication Method** is **Shared Secret**, the right dialog box is used.

3. Edit or complete the appropriate fields from either dialog box as follows:

Field Name	*Definition*
Connector Name	Name of the VPN connection.
Authentication Protocol	Authentication protocol used to establish a VPN connection.
Authentication Method	Authentication method used to establish a VPN connection.

Field Name	*Definition*
Remote ("Right")	
ID	The identification name of the remote host, commonly referred to as the "right" host.
IP Address	Remote IP address.
NextHop	The router to which the Console Server sends packets in order to deliver them to the left.
Subnet Mask	As indicated.
RSA Key	You may use the copy and paste feature of your browser to enter the RAS key.
Local ("Left")	
ID	The identification name of the local host, commonly referred to as the "left" host.
IP Address	The IP address of the local or left host.
NextHop	The router to which the Console Server sends packets in order to deliver them to the right.
Subnet Mask	As indicated
RSA Key	You may use the copy and paste feature of your browser to enter the RSA key.
Boot Action	The boot action configured for the local host.
Pre-Shared Secret	Pre-shared password between left and right users.

4. Select the **OK** button when done.
5. Select the **Apply Changes** button to save your configuration.

Network > SNMP

Short for Simple Network Management Protocol, SNMP is a set of protocols for managing complex networks. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network. SNMP-compliant devices (*agents*), store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

The KVM/net uses the Net-SNMP package (http://www.net-snmp.org). The Net-SNMP package contains various tools relating to the Simple Network Management Protocol including an extensible agent, an SNMP library, tools to request or set information from SNMP agents, tools to generate and handle SNMP traps, a version of the unix 'netstat' command using SNMP and a Tk/perl mib browser.

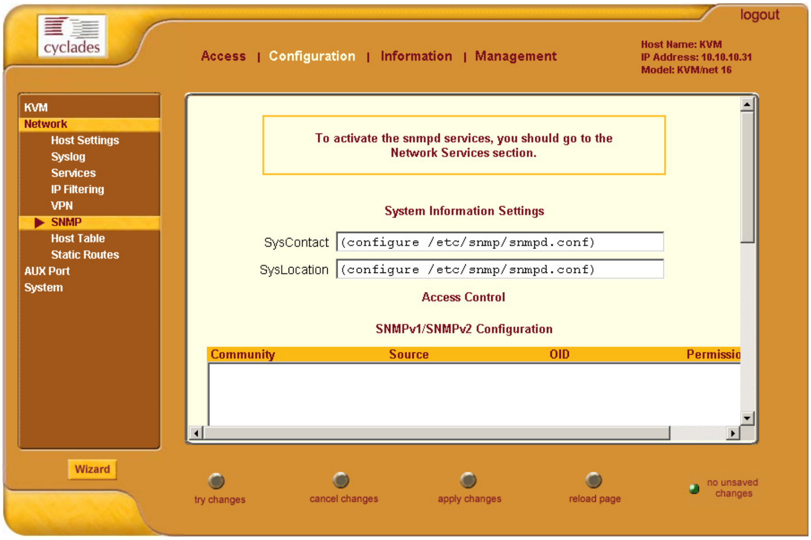
SNMP is configured with community names, OID and user names. The KVM/net supports SNMPv1, v2 and v3. The two versions require different configurations. SNMPv1/v2 requires community, source, object ID and the type of community (read-write, read-only). V3 requires user name.

Important! *Check the SNMP configuration before gathering information about KVM/net by SNMP. There are different types of attacks an unauthorized user can implement to retrieve sensitive information contained in the MIB. By default, the SNMP configuration in KVM/net cannot permit the public community to read SNMP information.*

To configure SNMP:

1. From the top menu bar, select **Networks**; from the left menu panel, select **SNMP Daemon Settings**.

   The system invokes the SNMP Daemon Settings form:



Host Name: KVM
IP Address: 10.10.10.31
Model: KVM/net 16

To activate the snmpd services, you should go to the Network Services section.

System Information Settings

SysContact (configure /etc/snmp/snmpd.conf)

SysLocation (configure /etc/snmp/snmpd.conf)

Access Control

SNMPv1/SNMPv2 Configuration

Community	Source	OID	Permissio

2. Type in the following System Information, as necessary:

Field Name	*Definition*
Community	The community name acts as a password to authenticate messages sent between an SNMP client and a router containing an SNMP server. The community name is sent in every packet between the client and the server.
SysContact	The email of the person to contact regarding the host on which the agent is running (e.g., me@mymachine.mydomain)
SysLocation	The physical location of the system (e.g., mydomain).

If you are using SNMPv3, skip steps 2 and 3; proceed to step 4.

3. To Add an SNMP agent using SNMPv1/SNMP2 Configuration, select the Add button located at the bottom of this view table.

   OR

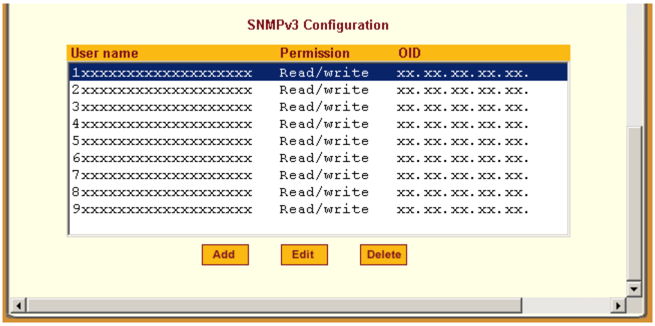
   To edit an SNMP agent, select the **Edit** button.

   The system invokes the New/Modify SNMP Daemon Configuration dialog box:

4. Complete the dialog box as follows:

Field Name	*Definition*
Community	The community name acts as a password to authenticate messages sent between an SNMP client and a router containing an SNMP server. The community name is sent in every packet between the client and the server.
Source	The source IP address or range of IP address.
OID	Object Identifier.
Permission	Select the permission type: Read Only - Read-only access to the entire MIB except for SNMP configuration objects. Read/Write - Read-write access to the entire MIB except for SNMP configuration objects. Admin - Read-write access to the entire MIB.

5. If you are adding or editing an SNMP agent using SNMPv3, scroll down to the lower half of the SNMP Configuration form:



SNMPv3 Configuration

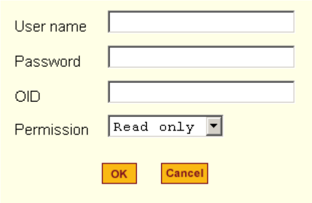
User name	Permission	OID
1xxxxxxxxxxxxxxxxxxxx	Read/write	xx.xx.xx.xx.xx.
2xxxxxxxxxxxxxxxxxxxx	Read/write	xx.xx.xx.xx.xx.
3xxxxxxxxxxxxxxxxxxxx	Read/write	xx.xx.xx.xx.xx.
4xxxxxxxxxxxxxxxxxxxx	Read/write	xx.xx.xx.xx.xx.
5xxxxxxxxxxxxxxxxxxxx	Read/write	xx.xx.xx.xx.xx.
6xxxxxxxxxxxxxxxxxxxx	Read/write	xx.xx.xx.xx.xx.
7xxxxxxxxxxxxxxxxxxxx	Read/write	xx.xx.xx.xx.xx.
8xxxxxxxxxxxxxxxxxxxx	Read/write	xx.xx.xx.xx.xx.
9xxxxxxxxxxxxxxxxxxxx	Read/write	xx.xx.xx.xx.xx.

6. To Add an SNMP agent using SNMPv3 Configuration, select the **Add** button located at the bottom of this view table.

   OR

   To edit an SNMP agent, select the Edit button.

   The system invokes the New/Modify SNMP Daemon Configuration dialog box.



User name

Password

OID

Permission Read only

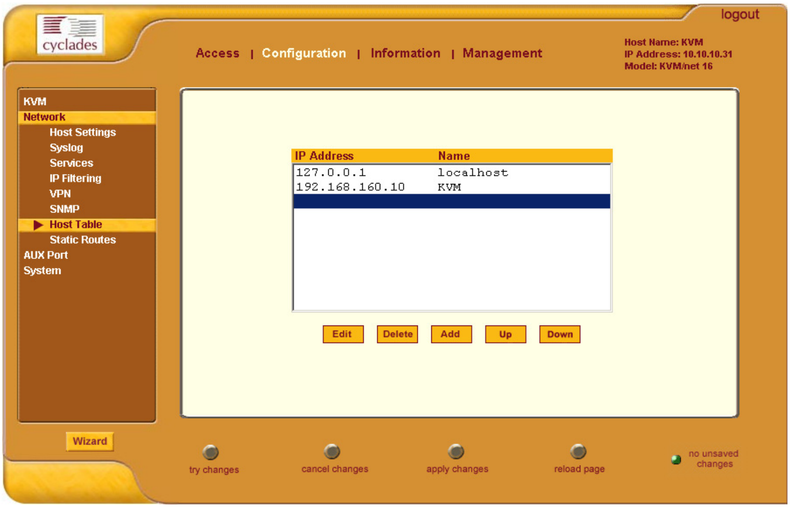
7. Complete the form and when done, select the **OK** button from the dialog box.
8. Verify your entry or modification from the respective tables of the SNMP Configuration form.
9. Select the **Apply Changes** button to complete the procedure.

Network > Host Table

The Host Tables form enables you to keep a table of host names and IP addresses that comprise your local network, and thus provide information about your network environment.

1. From the top menu, select **Network**; from the left menu, select **Host Table**.

   The system invokes the Host Table form:



Host Name: KVM
IP Address: 10.10.10.31
Model: KVM/net 16

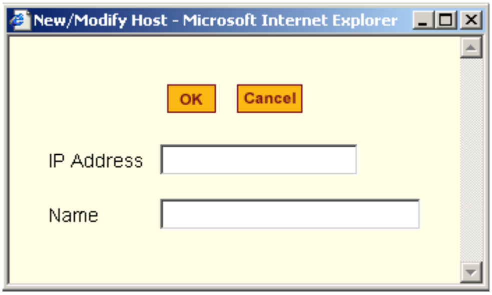
IP Address	Name
127.0.0.1	localhost
192.168.160.10	KVM

2. To edit host, select the host IP address from the Host Table and then click on the **Edit** button. (If the list is long, use the **Up** and **Down** buttons to go through each item in the list.)

   - OR -

   To add a host, click the **Add** button.

   The system brings up the following dialog box:



3. Type in the new or modified host address in the **IP Address** field, and the host name in the **Name** field, and then select the **OK** button.
4. To delete a host, select the host you wish to delete from the Host Table form, and then select the **Delete** button from the form.
5. Select the **Apply Changes** button to save your configuration to Flash.

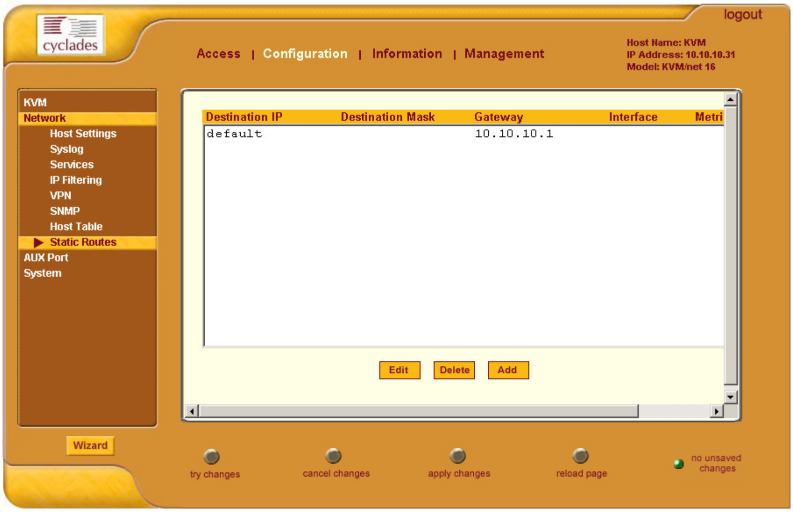
Network > Static Routes

The Static Routes form allows you to manually add routes. The Routing Table defines which interface should transmit an IP packet based on destination IP information. Static routes are a quick and effective way to route data from one subnet to another.

You can add or edit a hard-coded static route by clicking on the corresponding buttons. They'll bring you to a dialog box to enter the route to be added. To delete a static route, highlight the route and select **Delete**.

1. From the top menu, select **Network**; from the left menu, select **Static Routes**.

   The system brings up the Static Routes table form:



Destination IP	Destination Mask	Gateway	Interface	Metri
default		10.10.10.1		

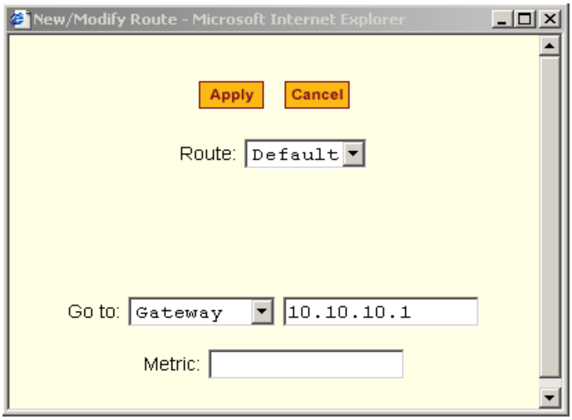
Refer to the field definitions in Step 3 for the meaning of each field in the table.

2. To edit a static route, select a route from the Static Routes form, and then select the **Edit** button.

   - OR -

   To add a static route, select the **Add** button from the form.

   The system invokes the **New/Modify Route** dialog box:



Route: Default

Go to: Gateway 10.10.10.1

Metric:

3. Complete the dialog box as follows:

Field Name	*Definition*
Route	Select **Default**, **Network**, or **Host**.
Network IP	*This field appears only if Network is selected.* The address of the destination network.
Network Mask	*Only if Network is selected.* The mask of the destination network.
Host IP	*Only if Host is selected.* The IP address of the destination host.
Go to	Select **Gateway** or **Interface**.
[*Adjacent field*]	The address of the gateway or interface.
Metric	The number of hops.

4. Select **Apply** when done.

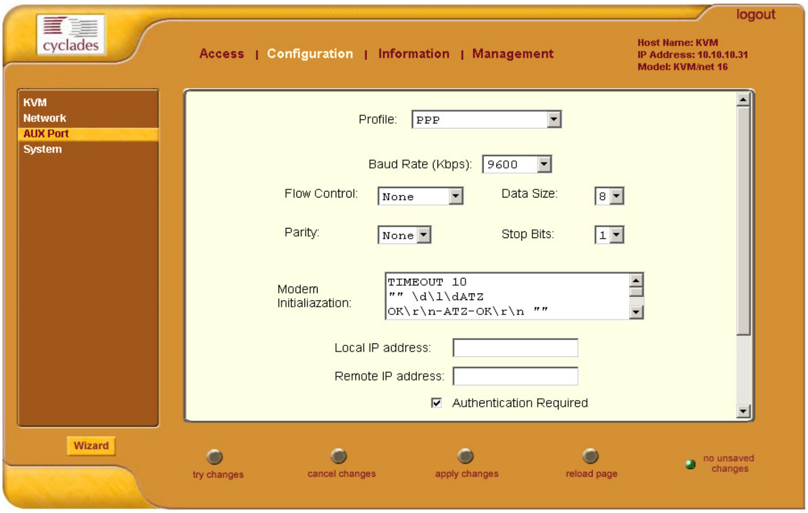
AUX Port

The **AUX**(iliary) **Port** form is used to configure the auxiliary port settings to suit the profile or the device to be connected (in this case, a modem or a power management) to the KVM/net unit.

1. From the top menu, select **Configuration**; from the side menu, select **AUX Port**.

   The system brings up the Auxiliary Port form.

   From the **Profile** field of the Auxiliary Port form, select Power Management or PPP. If you select PPP, the following additional fields will appear on the form:



Host Name: KVM
IP Address: 10.10.10.31
Model: KVM/net 16

Profile: PPP

Baud Rate (Kbps): 9600

Flow Control: None

Data Size: 8

Parity: None

Stop Bits: 1

Modem Initialiazation:

```
TIMEOUT 10
"" \d\l\dATZ
OK\r\n-ATZ-OK\r\n ""
```

Local IP address:

Remote IP address:

☑ Authentication Required

2. To configure the Aux Port for PPP, complete the fields as shown below and select **Apply Changes** when done.

Field Name	*Definition*
Profile	Select the device to be connected. For **PPP**, the following input fields are used:
Baud Rate	The port speed.
Flow Control	Gateway or interface address used for the route.
Data Size	The number of data bits.
Parity	None, even or odd.
Stop Bits	The number of stop bits.
Modem Initialization	The modem initialization string.
Local IP Address	The 32-bit local IP address.
Remote IP Address	The 32-bit remote IP address
Authentication Required	Select checkbox if authentication is required.
MTU/MRU	The maximum transmission unit / maximum receive units for the PPP.
PPP Options	The options for this protocol.

System

The **System** menu, which is the fourth selection under the **Configuration** menu, comprises two forms: **Date/Time** and **Boot**.

System > Date/Time

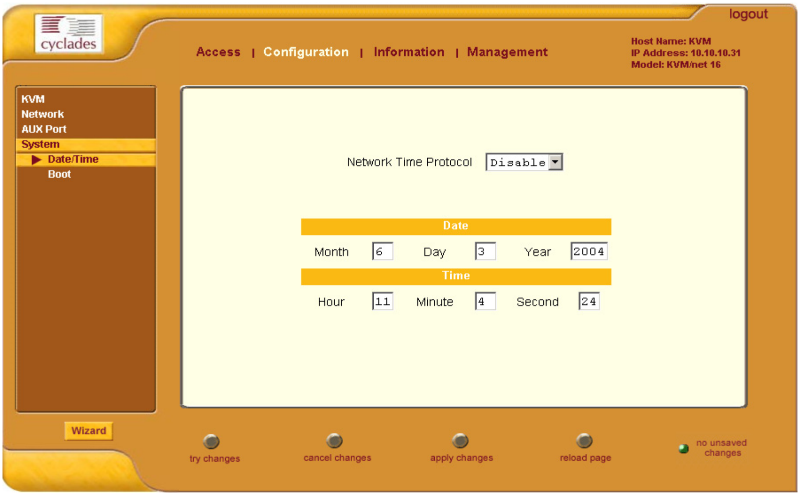
The Time/Date form is used to enable the KVM/net to work as an NTP client, synchronizing your system clock with the *true time* (*i.e.*, the average of many high-accuracy clocks around the world. By default, NTP is disabled; you may enter the time and date manually using the Time/Date form.

Manual Setting

To set time and date manually, perform the following steps:

1. From the top menu, select **Configuration**; from the left menu, under **System**, select **Time/Date**.

   The system brings up the **Time/Date** form:



Host Name: KVM
IP Address: 10.10.10.31
Model: KVM/net 16

Network Time Protocol: Disable

Date

Month	6	Day	3	Year	2004

Time

Hour	11	Minute	4	Second	24

2. If you are not using NTP, complete the date and time fields by selecting the appropriate numbers from the dropdown list boxes.
3. Click on the **Apply Changes** button to complete the procedure.

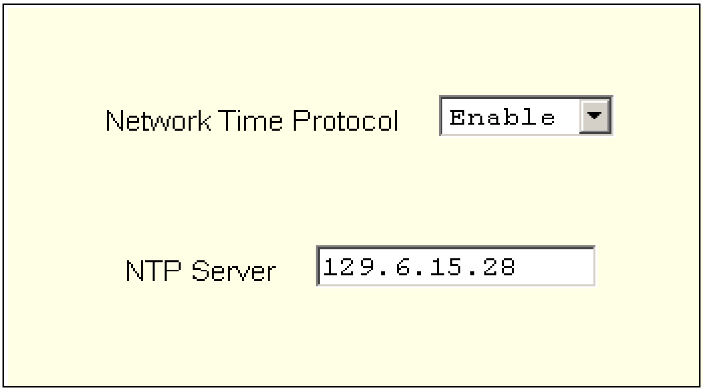
NTP Setting

To set the time and date through NTP, perform the following steps:

1. Choose **Enable** from the **Network Time Protocol** field of the Date/Time form.

   The system invokes the **NTP Server** field.

2. Type in the address of the NTP server in the **NTP Server** field.



Network Time Protocol: Enable

NTP Server: 129.6.15.28

3. Click on the **Apply Changes** button.

System > Boot

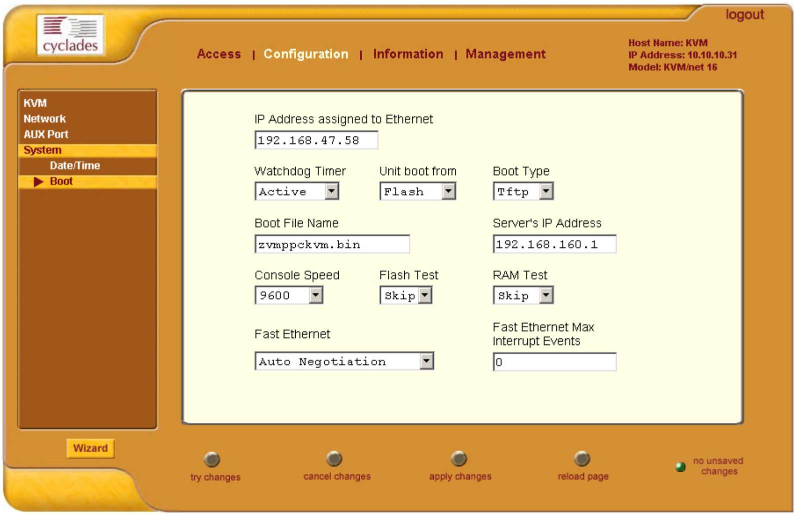
Boot configuration defines the settings for loading the operating system.

The KVM/net can boot from its internal firmware or from the network. By default, the unit boots from Flash. If you need to boot from the network, install one TFTP or BOOTP server with the firmware to boot from, and then choose **boot from network** and fill in the fields. You may skip Flash test and RAM test for a faster boot.

To configure the KVM/net boot settings:

1. From the top menu bar, select **Configuration**; from the left menu panel, under **System**, select **Boot Configuration**.

   The system brings up the Boot Configuration form:



Host Name: KVM
IP Address: 10.10.10.31
Model: KVM/net 16

IP Address assigned to Ethernet: 192.168.47.58

Watchdog Timer: Active

Unit boot from: Flash

Boot Type: Tftp

Boot File Name: zvmppckvm.bin

Server's IP Address: 192.168.160.1

Console Speed: 9600

Flash Test: Skip

RAM Test: Skip

Fast Ethernet: Auto Negotiation

Fast Ethernet Max Interrupt Events: 0

2. Complete the fields as follows:

Field Name	*Definition*
IP Address assigned to Ethernet	As indicated.
Watchdog Timer	Sets the Watchdog Timer to Active or Inactive.
Unit boot from	Specify whether to boot unit up from Flash or from the Network.
Boot Type	Select from the following types of booting: bootp, tftp, or both.
Boot File Name	Filename of the boot program you want to use.
Server’s IP Address	As indicated.
Console Speed	Select from: 4800 through 118200.
Flash Test	Select this to test boot from the Flash card. You can Skip this test, or do a Full test.

Field Name	*Definition*
RAM Test	Select this to test boot from RAM. You can Skip this test, do a Quick test or a Full test.
Fast Ethernet	Select the appropriate Ethernet setting if you need to change the Auto Negotiation (default value): 100BaseT Half-Duplex 100BaseT Full-Duplex 10BaseT Half-Duplex 10BaseT Full-Duplex
Fast Ethernet Max. Interrupt Events	The maximum number of packets that the CPU will handle.

3. Select **Apply Changes** to save your configuration to Flash.

Information

The **Information** menu provides two forms for viewing information:

- General
- Port Status

General

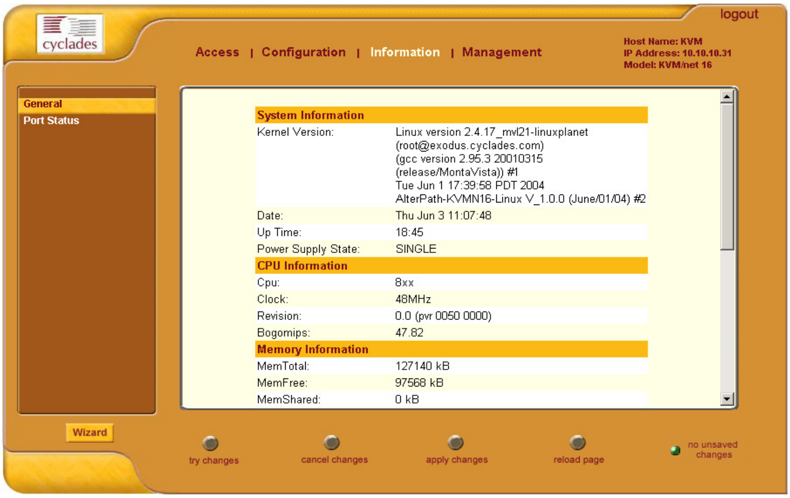
Use the General form to view system information in the following categories:

- System (e.g., Kernel version, Date, Uptime, etc.)
- CPU
- Memory
- Ram Disk Usage
- Fan Status

To view General information:

1. From the top menu, go to **Information**; from the side menu, select **General**.

   The system brings up the following view form:



Host Name: KVM
IP Address: 10.10.10.31
Model: KVM/net 16

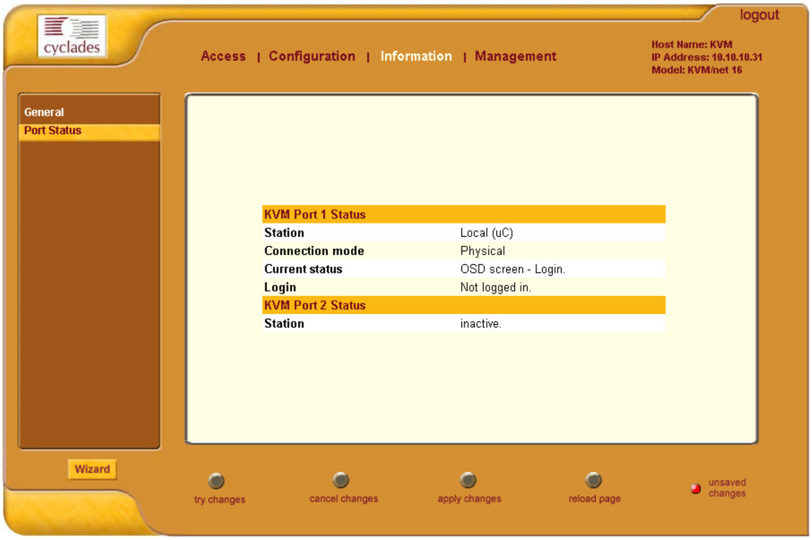
System Information	
Kernel Version:	Linux version 2.4.17_mvl21-linuxplanet (root@exodus.cyclades.com) (gcc version 2.95.3 20010315 (release/MontaVista)) #1 Tue Jun 1 17:39:58 PDT 2004 AlterPath-KVMN16-Linux V_1.0.0 (June/01/04) #2
Date:	Thu Jun 3 11:07:48
Up Time:	18:45
Power Supply State:	SINGLE
CPU Information	
Cpu:	8xx
Clock:	48MHz
Revision:	0.0 (pvr 0050 0000)
Bogomips:	47.82
Memory Information	
MemTotal:	127140 kB
MemFree:	97568 kB
MemShared:	0 kB

Port Status

Use the Port Status form to view the system status of each KVM/net port.

1. From the top menu, select **Information**; from the side menu, select **Port Status**.

   The system brings up the **Port Status** view form:



KVM Port 1 Status	
Station	Local (uC)
Connection mode	Physical
Current status	OSD screen - Login.
Login	Not logged in.
KVM Port 2 Status	
Station	inactive.

Management

The Management menu comprises seven forms relating to system and software management such as booting, backing up, and handling configuration data.

Menu Selection	*Use this menu to:*
Backup Configuration	Use a FTP server to save or retrieve your configuration data.
Firmware Update	Upload firmware from the web to the KVM/net and save the new software version or update.
Microcode Update	Update any of the micro controller microcodes that are stored in the KVM terminator, main KVM/net, local KVM/net, and internal KVM/net switch.
Microcode Reset	Reset any of the micro controller microcodes.

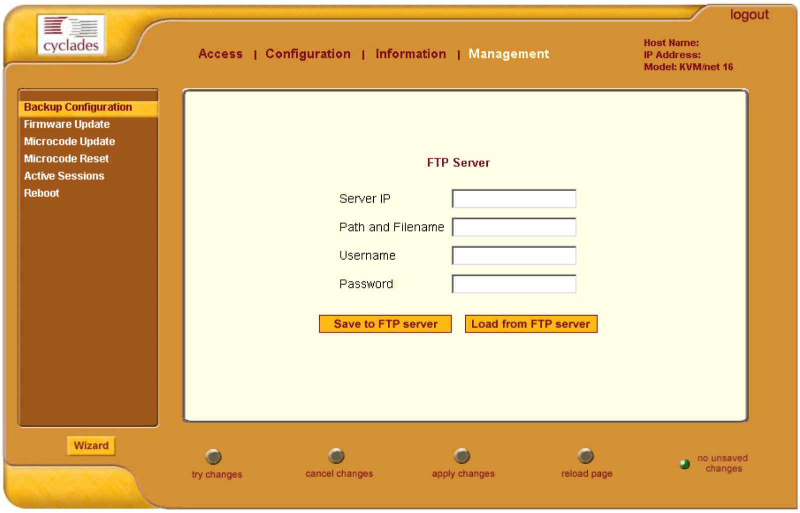
Menu Selection	*Use this menu to:*
Active Sessions	View the status of all active sessions as well as reset or kill sessions.
Reboot	Reboot the system.

Backup Configuration

The Backup Configuration form allows you to set the KVM/net to use a FTP server to save and retrieve its configuration. For the backup configuration to work, the FTP server must be on the same subnet. Ensure that it is accessible from the KVM/net by pinging the FTP server.

1. From the top menu, select **Management**; from the left menu, select **Backup Configuration**.

   The system brings up the **Backup Configuration** form:



2. Complete the fields and then select one of the following buttons:
   - **Save to FTP server** - select this if you want to save your configuration to the FTP server.
   - **Load from FTP server** - select this if you want to load your configuration from the FTP server to the KVM/net.

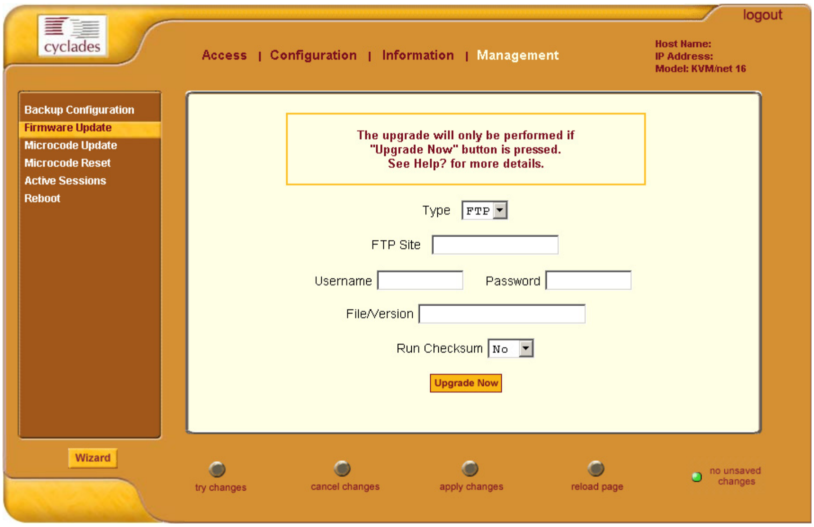
3. Select the **Apply Changes** button when done. The configuration loaded should run after a reboot.

Firmware Update

To upgrade your KVM/net firmware, perform the following steps:

1. From the top menu, select **Management**; from the side menu, select **Firmware Update**.

   The system brings up the Firmware Update form:



The upgrade will only be performed if "Upgrade Now" button is pressed. See Help? for more details.

Type: FTP

FTP Site

Username

Password

File/Version

Run Checksum: No

2. From the Firmware Update form, complete the fields as follows:

Field Name	*Definition*
Type	The method of upload.
FTP Site	The address of the FTP site.
Username	Username of the person who is doing the upload.
Password	Password associated with the Username.
File Version	The firmware file version.
Run Checksum	Runs the checksum program to verify the accuracy of the uploaded data.

3. Select the **Upgrade Now** button.
4. Select the **Apply Changes** button at the bottom of the configuration window.

Microcode Update

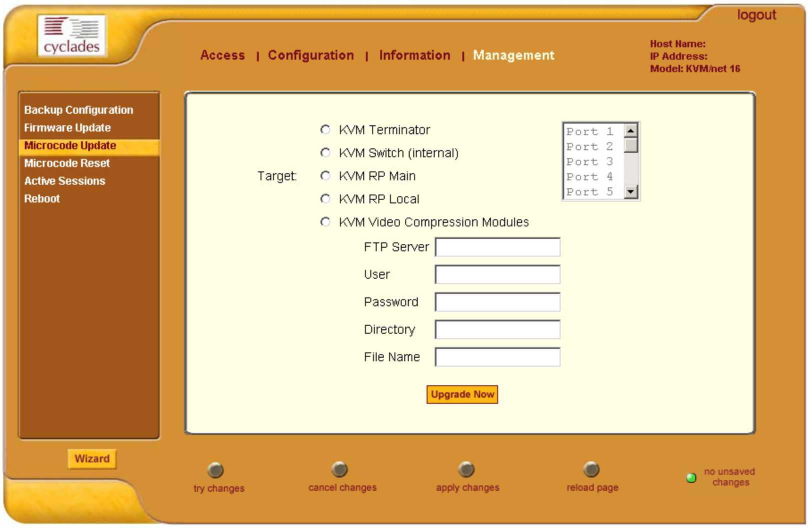
Through an FTP server, the Microcode form is used to update any of the micro controller microcodes that are stored separately in each of the following target locations:

- KVM Terminator
- KVM Switch (internal)
- KVM Main
- KVM Local

To update a microcode:

1. From the top menu, select **Management**; from the side menu, select **Microcode Update**.

   The system brings up the Microcode form:



2. Complete the input fields as follows:

Field Name	*Definition*
Target	The specific KVM microcode that you wish to update (i.e., KVM Terminator, KVM Switch (internal), KVM Main, and KVM Local).
FTP server	Address of the FTP server used to update the microcode.

Field Name	*Definition*
User	The authorized user name.
Password	The user’s password.
Directory	Location (directory path) of the microcode file.
Filename	The microcode filename.

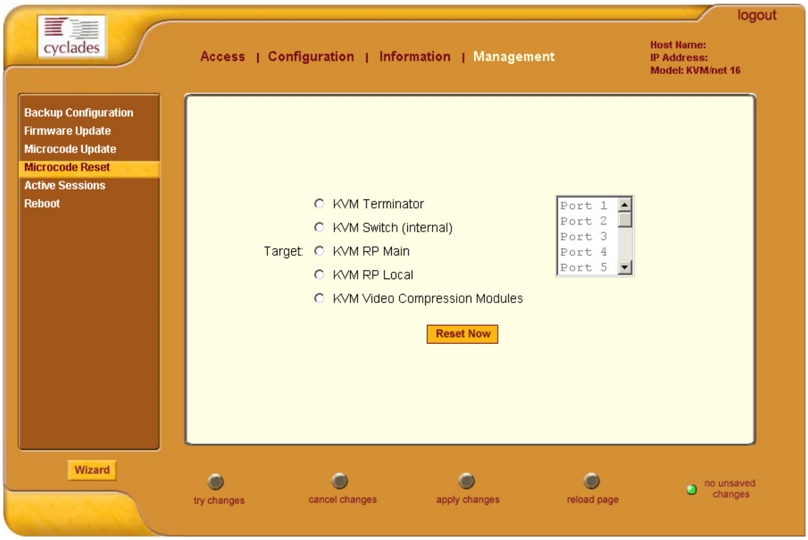
3. From the scrollable port list, select the port to which the target is connected.
4. Select the **Upgrade Now** button.

Microcode Reset

The Microcode Reset form is used to reset the hardware associated with the afore-discussed microcodes.

1. From the top menu, select **Management**; from the side menu, select **Microcode Reset**.

   The system brings up the Microcode Reset form:



2. From the form select the microcode or hardware target.
3. From the scrollable port list, select the port to which the target is connected, and then select the **Reset Now** button.

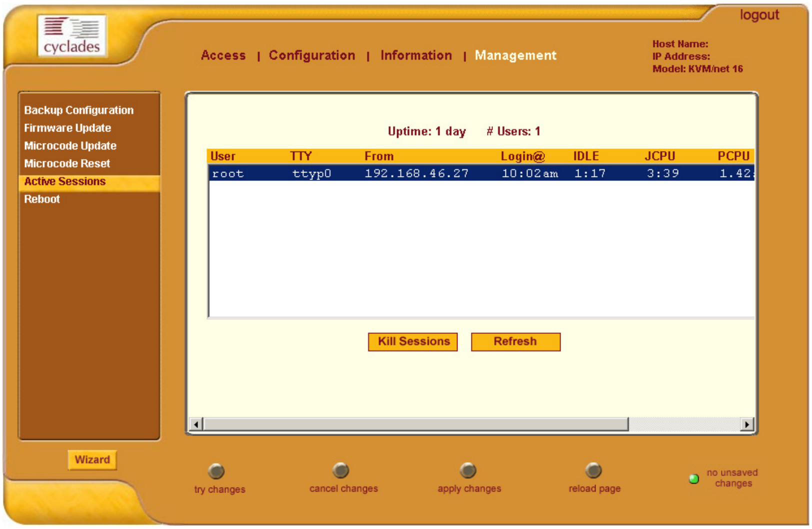
Active Sessions

The Active Sessions window is designed to provide you a quick status, and usage information (*e.g.*, user, tty, Login time, JCPU, *etc*.) pertaining to all active server sessions. You may also kill or refresh a session.

Open sessions are displayed with their identifications and statistics data for login, session and CPU usage for the specific client. JCPU relates all processes attached to that port including running background processes. PCPU relates the current processing time.

1. From the top menu bar, select **Management**; from the left menu panel, select **Active Sessions**.

   The system invokes the Active Sessions window:



Uptime: 1 day # Users: 1

User	TTY	From	Login@	IDLE	JCPU	PCPU
root	ttyp0	192.168.46.27	10:02am	1:17	3:39	1.42

What the heading and column name means:

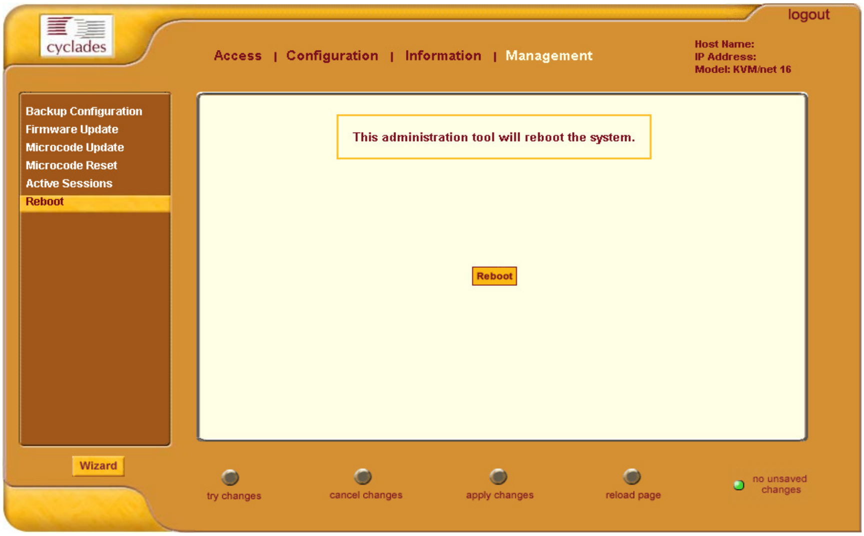
Field / Column	*Definition*
Uptime	System uptime in minutes and seconds (mm:ss).
# Users	Number of current users.
User	The user who initiated the session.
TTY	The name of the serial port.
From	The network machine to which the port is connected.

Field / Column	*Definition*
Login@	The day and time of the last login.
Idle	The time when the session or server became inactive.
JCPU	The duration of time used by all processes attached to the tty. It does not include past background jobs; only currently running background jobs.
PCPU	The time used by the current process that is named in the What column.
What	The current process attached to the tty.

2. To kill or refresh a session, select from the Active Sessions view table the session you wish to delete or refresh.
3. Click on the **Kill Session** or **Refresh** button.
4. From the configuration window, click on the **Apply Changes** button.

Reboot

The Reboot form allows you to reboot the system by clicking the **Reboot** button (go to **Management** > **Reboot**) as shown:


This administration tool will reboot the system.

Chapter 4
KVM/net Operation

Addressed to the regular user, this chapter presents the procedures and requirements for operating the AlterPath KVM/net, and is organized as follows:

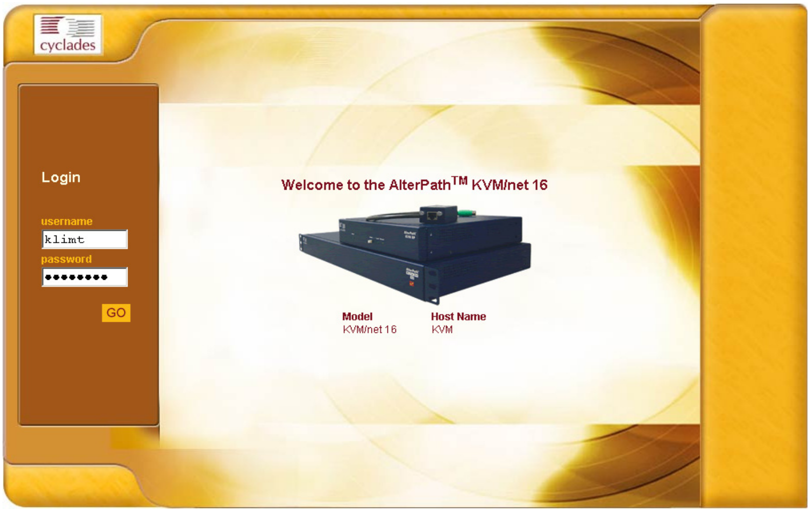
- Logging in
- KVM/net Web Management Interface
- AlterPath Viewer: Connection Menu
- KVM/net Viewer Navigation Keys
- Default Key Sequences
- Changing Your Password
- Connecting to a Server
- Cycling Between Servers
- Remote Operation
- Operating through the Remote Unit (RP)
- Adjusting Screen Brightness and Contrast
- Sharing Server Connection
- Synchronizing Keyboard and Mouse
- Establishing a Power Control Session
- Power Management

For procedures on how to log in and operate the KVM/net as an administrator, refer to ***Chapter 3: KVM/net Configuration****.*

Logging In

1. Connect your internet browser to the KVM/net application by typing in the KVM/net server's IP address (*e.g.*, http://10.0.0.0) in the browser's address (URL) field.

   The system brings up the AlterPath KVM/net **Login** screen:



Login

username
klimt

password
••••••••

Welcome to the AlterPath^{TM} KVM/net 16

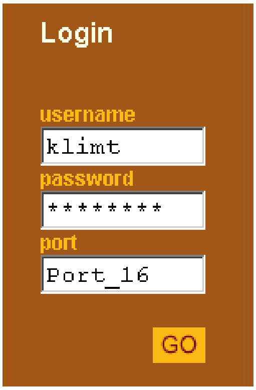
Model
KVM/net 16

Host Name
KVM

2. Log in your User Name and Password as provided to you by your system administrator, and then press <Enter> or select **Go**.

   The system invokes the **Connect** form.

3. If the **Login** screen has been configured to allow direct access to a port, you may enter the port number in the additional **port** field as shown:



Login

username
klimt

password
****

port
Port_16

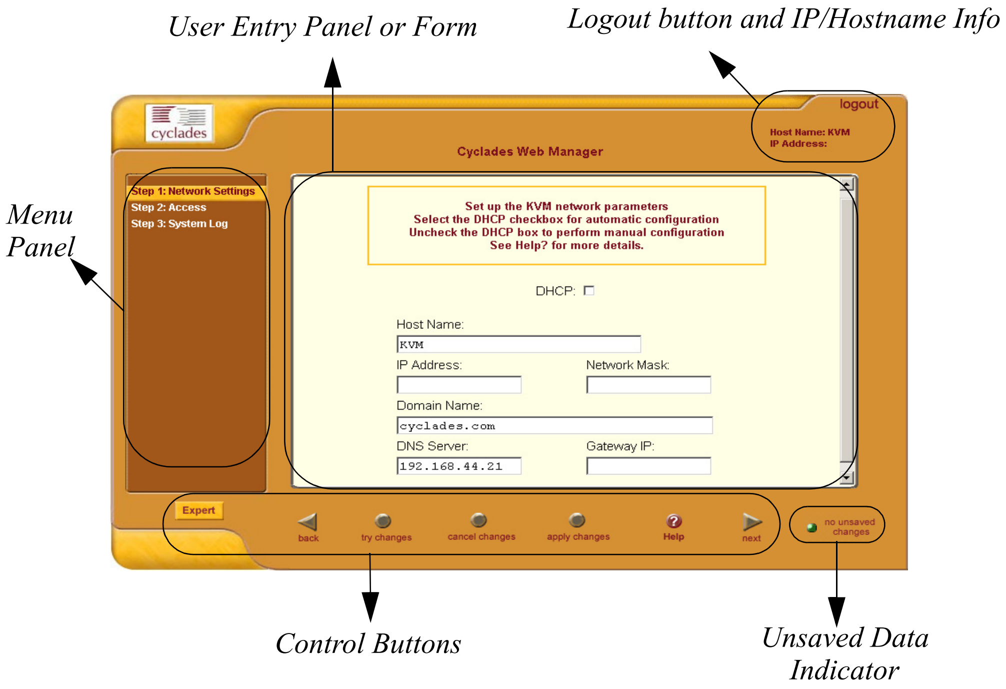
The **port** field accepts either the port alias or the port number using the following format: **port**_[port number].

Example: **Port_8**

IMPORTANT: *Take note of this login procedure. All subsequent online procedures in this chapter will assume that you are already logged in.*

KVM/net Web Management Interface

Before continuing, take some time to familiarize yourself with the application's GUI elements. The window shown below is for illustration purposes only; it is not the first window that you will see when you log in to the KVM/net.



Host Name: KVM
IP Address:

Set up the KVM network parameters
Select the DHCP checkbox for automatic configuration
Uncheck the DHCP box to perform manual configuration
See Help? for more details.

DHCP: □

Host Name: KVM

IP Address:

Network Mask:

Domain Name: cyclades.com

DNS Server: 192.168.44.21

Gateway IP:

The user interface provides you with a main menu and a set of control buttons located at the bottom of the application window. The user entry panel or form changes based on your menu selection.

When you click the **Connect** button (from the **Connect** form) to connect to a server, the system will launch the AlterPath KVM/net Viewer and connect to the server. The very first time the system invokes the Viewer, it will prompt you to accept a Security Certificate.

Once connected you can connect to another server by typing in <Ctrl-K> and then <Q> to call the **Connection Menu** which will allow you to switch to another server.

Connecting to a Server

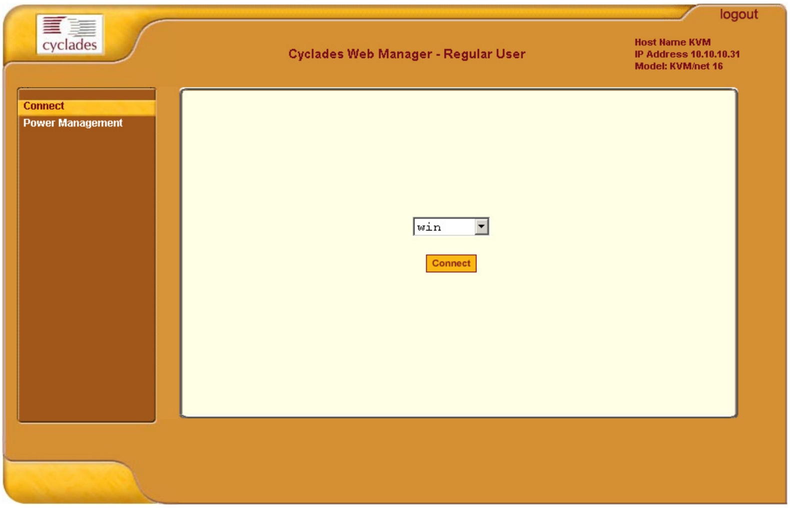
The **Connect** form is used to:

- Launch the KVM/net viewer and connect to a server based on your port selection from the drop down list box.
- Manage the servers from the viewer through the Connection Menu, using the key sequences and navigation keys.

In each case the KVM/net launches a java browser to make the connection.

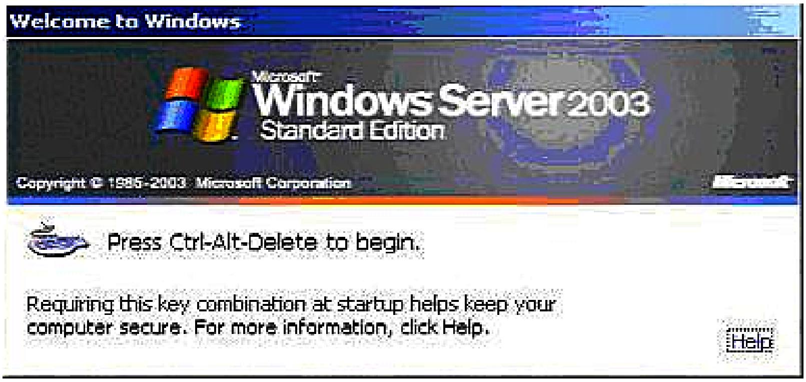
1. From the left menu panel, select **Connect**.

   The system invokes the Port Connection form:



2. From the drop down menu, select the port to which you want to connect.
3. Click on the **Connect** button.

The system launches the KVM/net viewer:



Welcome to Windows

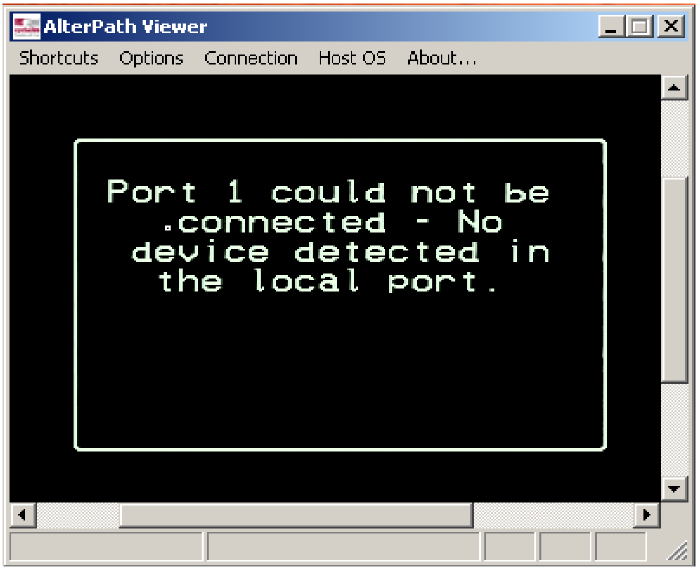
Microsoft Windows Server 2003 Standard Edition

Copyright © 1985-2003 Microsoft Corporation

Press Ctrl-Alt-Delete to begin.

Requiring this key combination at startup helps keep your computer secure. For more information, click Help.

If there is no device connected, the viewer responds with the following message:



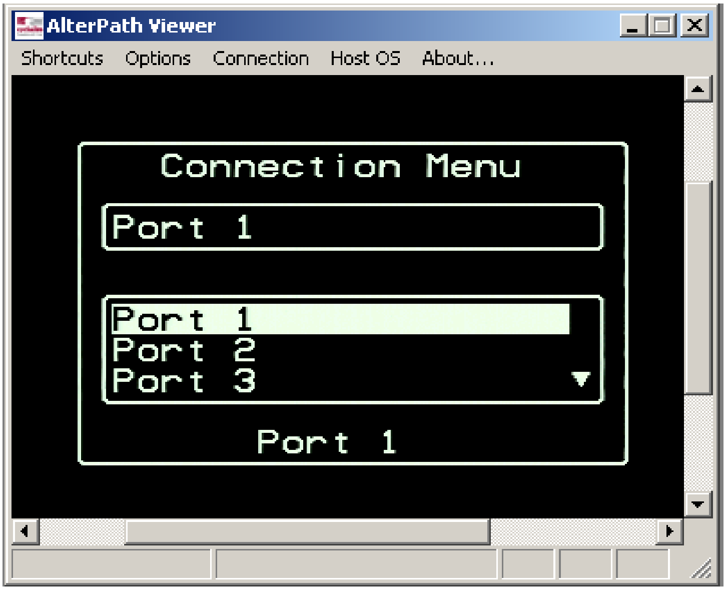
Port 1 could not be .connected - No device detected in the local port.

4. Press <Ctrl-K> and then <Q> to close the port session and invoke the **Connection Menu**.

AlterPath Viewer: Connection Menu

Once you have launched the AlterPath Viewer, you can connect to any server through the Connection Menu. The menu allows you to:

- Connect to a Port
- Exit from the Viewer



Refer to the succeeding sections on Overlaying Connection Menu: Navigation Keys and Default Key Sequences to ensure full use of the viewer.

Overlaying Connection Menu: Navigation Keys

Below is a short list of keyboard controls to help you navigate through the KVM Viewer. For the keys to work, make sure that your window is selected so that it is in the *active* state.

Key	*Action*
TAB	Changes between fields on the window.
UP / DOWN ARROW	Scrolls within a menu.
BACKSPACE	Deletes character left to the cursor.

Key	***Action***
PAGE UP / PAGE DOWN	Skips to the third line.
END	Moves to the end of a menu
HOME	Moves to the top of a menu
ENTER	Selects highlighted item; Commits changes

Default Key Sequences

A *key sequence* (also known as *escape sequence*) is a sequence of special characters used to send a command to a device or program, in this case the KVM/net application. Typically, an escape sequence begins with an escape character (hence, the term), but this is not universally true.

In KVM/net, the default key sequence (Ctrl-K, Q) for getting out of a particular window while connected to a port is also called *escape sequence*.

Aside from the navigation keys listed above, you can use the following key sequences to perform a specific action:

Key Sequence	***Action***
Ctrl-K and then **Q**	Quit command - closes the port session and returns to the KVM/net Main Menu.
Ctrl-K and then **P**	Port command - initiates a power control session.
Ctrl-K and then **C**	KVM Switch command - starts the continuous cycling of all authorized ports. This function is available only to the local user.
Ctrl-K and then **V**	Video command - controls screen brightness and contrast.
Ctrl-K and then **S**	Keyboard and Mouse Synchronization command - resets the keyboard and mouse synchronization if either one becomes unavailable after adding a new server to the KVM/net.
Ctrl-K . (period)	Next Port command - moves from the currently connected port to the next authorized port.
Ctrl-K , (comma)	Previous Port command - returns to the previous port.

Changing Your Password

If you are a system administrator or a user with admin privileges, you can change your password by using the Command Line Interface (CLI).

1. Connect your PC terminal to the console port of your AlterPath KVM/net
2. Configure your COM port as follows:

   Serial Speed: 9600 bps

   Data Length: 8 bits

   Parity: None

   Stop Bits: 1 stop bit

   Flow Control: None

   ANSI emulation
3. Open your terminal emulation application (HyperTerminal, Kermit, or Minicom).
4. Log in as: **root** Password: **Cyclades**
5. Upon system prompt, enter the command: **passwd**
6. Type in your new password when prompted.
7. Save your new password to Flash by typing in: **saveconf**
8. Close your terminal session.

You may also change your password through the KVM/net configuration interface by referring to **Chapter 3: KVM/net Configuration**.

Differences in OSD Functions

The Online Screen Display (OSD) which also displays the overlaying menus is accessible to both local and remote users. There are, however, two main differences in the OSD features or functions for each user.

- Only the local user has access to the OSD Login screen.
- Only the local user can cycle between servers using the overlaying Connection Menu. (Consequently, only the local user can use the Ctrl-K keys to cycle)

How to Read the Port Numbers

The number enclosed in parenthesis following the port logical number is the physical port number.

Example: Server 2 (1)
Where: Server 2 = port name
1 = physical port number

A name and a number connected by a period (.) indicate the slave KVM followed by its physical port.

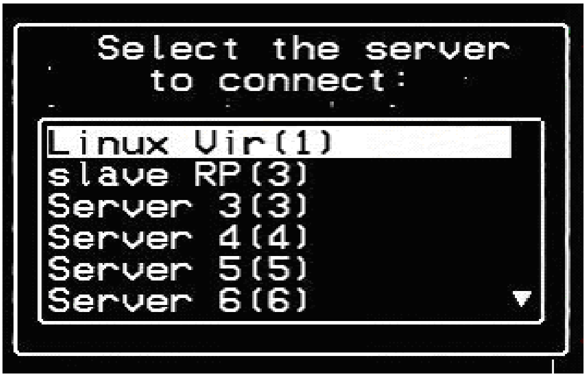
Example: kvm2.4
Where: kvm2 = slave name
4 = physical port on slave kvm2

How Server Names are Listed

A server does not need to have a name other than the logical/physical port number to which the server is connected. When a name has been assigned to a server, the name replaces the logical/physical port number in the Server Selection Menu.

If all servers were configured by their names, then the names are still sorted by physical port number.

In the sample Server Selection Menu below, you know that a server named **Linux Vir** is using Port 1.

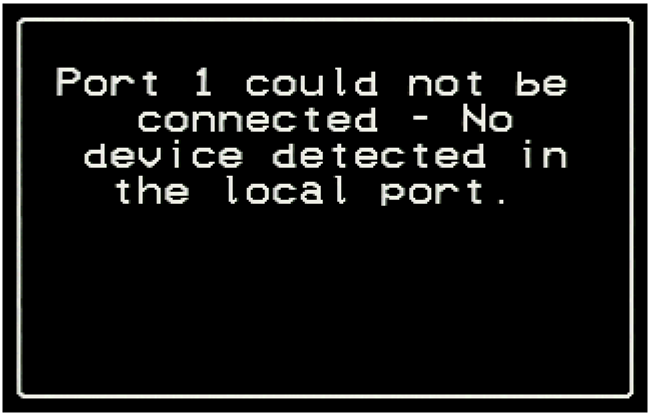


```
  Select the server
    to connect:

Linux Vir(1)
slave RP(3)
Server 3(3)
Server 4(4)
Server 5(5)
Server 6(6)       ▼
```

Cycling Between Servers

Cycle refers to the capability to access or connect from one authorized server to another. This feature is available to local the user only. Through the on-screen display interface, or by using a key sequence, KVM/net provides you immediate access to all connected or authorized servers. Cycling occurs in the order by logical port as they appear in the Server Connection Menu. In the cycle process, if there is no device attached to the port associated with the next logical port, a message will appear to indicate that there is no device connected:



```
Port 1 could not be
  connected - No
 device detected in
   the local port.
```

There are two types of cycle commands:

- Cycle by Server
- Cycle by Key Sequence

Cycle by Server enables you to view all authorized servers on a continuous basis until all server have been exhausted and then start over again. The cycle does not stop unless you enter the escape sequence (default: **Ctrl-K**, **Q**) to abort the process and close the session.

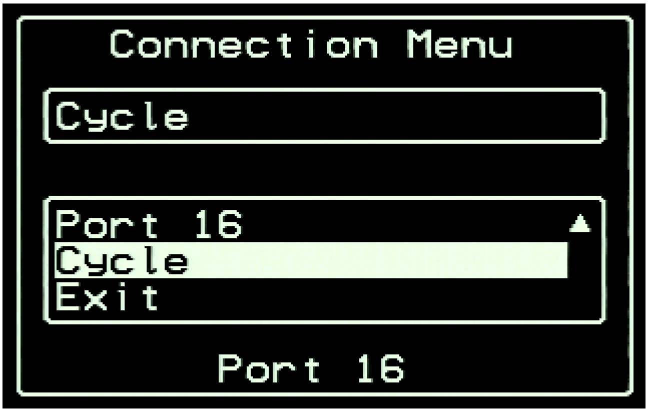
Cycle by Key Sequence allows you to view or access the next server by entering the Cycle key sequence (default: **Ctrl-K**, **C**). The procedure allows you to move from one server to the next authorized server, using one key sequence at a time.

Cycle by Server

To initiate Cycle by Server:

1. From the Connection Menu, choose **Cycle** and press **Enter**.

   The system brings up the Server Selection Menu:



The Cycle selection is available only to the local user, not the remote user.

2. Select **Cycle** (you may have to use the **End** key to find Cycle at the bottom of the list) from the Server Connection Menu and then press Enter.

   The system initiates cycle from the first authorized server.

Cycle by Key Sequence

The cycle by key sequence, like all key sequences, will work only when you are already viewing or accessing a server.

1. To access the next authorized server from the current server selection, press **Ctrl-K** followed by the **C** key.

   The system should take you to the next authorized server.

The key sequence for cycling (*Ctrl-K,C*) *works only if you are a local user.*

Using the KVM RP to Extend Operation

You can extend the local distance of your AlterPath KVM/net by using the AlterPath KVM RP. KVM/net supports two concurrent users through any combination of the following:

- One local user at the KVM/net switch.
- One extended user at the AlterPath RP location.
- One remote user over IP.

The AlterPath RP may be placed up to 500 feet away from the KVM/net unit, enabling the extended user to select the local keyboard, video, and mouse console between a local station and a server connected to the KVM/net.

*See **Chapter 2: KVM/net Installation** for details on how to install the AlterPath KVM RP.*

Operating through the Remote Unit (RP)

You can select the keyboard, video, and mouse extended console between a local station and a server connected to the KVM/net using any of the following methods:

- Press the button at the AlterPath KVM RP unit to switch the local video display between a local station and a server connected to the KVM/net.
- Use the key sequence [Scroll Lock] + [Scroll Lock] + R to switch the local video display to the remote server connected to the KVM/net.
- Use the key sequence [Scroll Lock] + [Scroll Lock] + L to switch the local video display to the local station connected to the KVM RP.

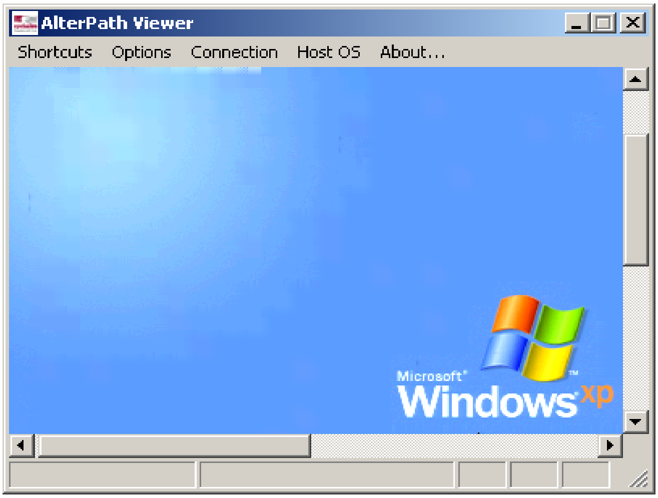
Finishing your Session

There are three ways to end your AlterPath Viewer session:

- Selecting **Exit** from the AlterPath Viewer Client
- Pressing the escape sequence (**Ctrl-K**, **Q**)
- Through Idle Timeout

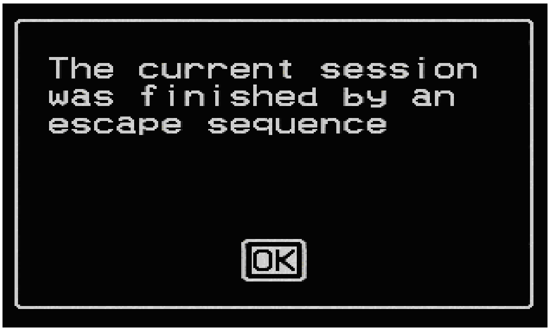
Method 1: Exiting from the AlterPath Viewer Client

From the menu bar of the AlterPath Viewer, go to: **Shortcuts** > **Exit Viewer Client**.



Method 2: Exiting by using the escape sequence.

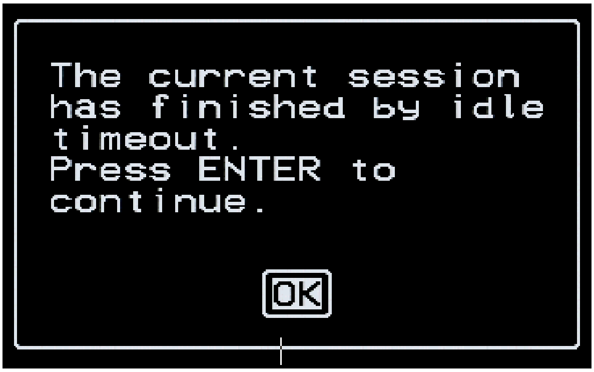
Press **Ctrl-K** keys followed by the **Q** key.
The system will close the session and send the following message:



The current session
was finished by an
escape sequence

Method 3: Exiting by Idle Timeout

Leaving your system idle will eventually close the session based on the configured idle time. When this happens, the system closes the session and sends the following message:



```
The current session
has finished by idle
timeout.
Press ENTER to
continue.
```

The idle time is set by the KVM/net administrator.

Adjusting Screen Brightness and Contrast

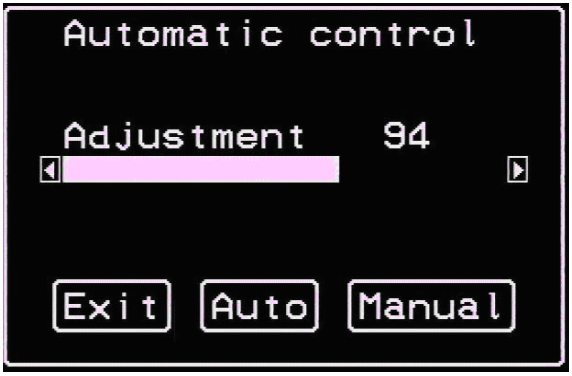
To adjust screen brightness, press the video control key sequence (**Ctrl-K** followed by the **V** key, default).

Depending on which window was accessed last, the system will display either one of the following overlaying windows:

- Automatic (Video) Control Adjustment
- Manual Brightness and Contrast Control

Automatic (Video) Control Adjustment

The Automatic Video Adjustment window is used to control the video signal input level to the KVM/net. This is used to compensate for the differences in video signal levels from the computers.

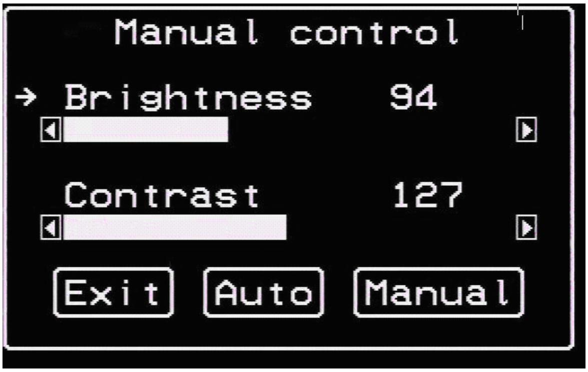


Adjustment 94

In the Automatic Control screen, press the <Tab> key to move from the Adjustment field to the **Exit**/**Auto**/**Manual** buttons. Once you are in one of the buttons, select the right or left arrows to move from one button to another.

Manual (Brightness/Contrast) Control

The Manual Control window is used to control the levels of video brightness and contrast. As in the Automatic Control overlay window, use the <Tab> key to move between the **Brightness**/**Contrast** fields and the **Exit**/**Auto**/**Manual** buttons.



→ Brightness 94

Contrast 127

Sharing Server Connection

The AlterPath KVM/net supports shared connections to a server. This feature is implemented based on the type of access permissions each of the users have for the specified server port.

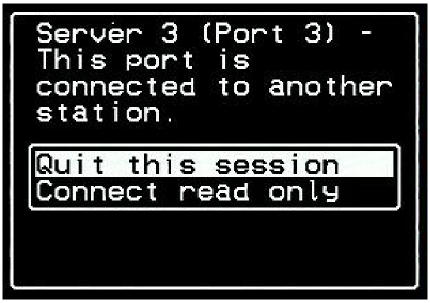
When a user connects to a server that is already in use, the software autodetects the event and presents a menu to the connecting user. Options available under this menu will vary depending on the connecting user access permissions. Also, a notification is presented to the current user, depending on the action selected by the connecting user. To better understand how this is done consider the following definitions:

- Read-only mode: session mode of a user with read-only permission for the server port
- Read-write mode: session mode of a user with read-write, read-write-config, read-write-power or full access permission for the server port

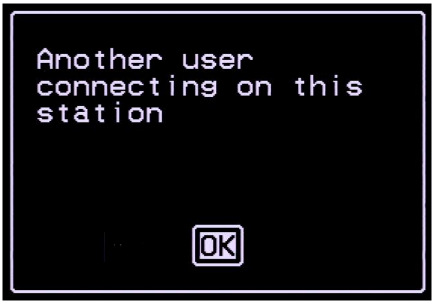
The following two options are always presented in the menu to the connecting user:

- Quit: Just quits the connection attempt and returns to the Server Connection Menu
- Connect read-only: connects the user in read-only mode and notifies the new connection to the previous user.

The menu presented to the connecting user and the notification message to the previous user are as follows:



Server 3 (Port 3) - This port is connected to another station.

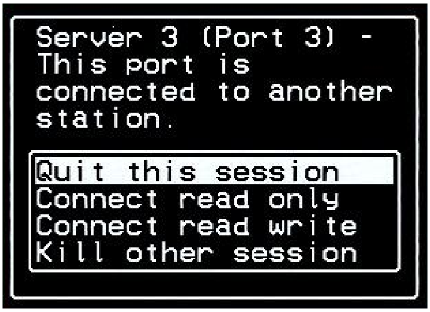


Another user connecting on this station

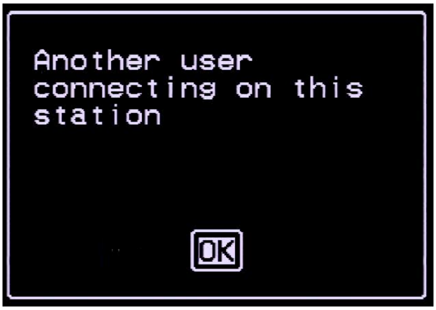
If the connecting user has either read-write, read-write-config, read-write-power or full access permission to the server port, the following additional options are presented in the menu:

- Connect read write: connects the user in read-write mode and the previous user is notified of the event. If the previous user is in read-write mode, its access mode is changed to read-only and he is notified of the event.
- Kill the other session: kills the existing session and connects the user in read-write mode. The previous user is notified of the event and is disconnected from the server port.

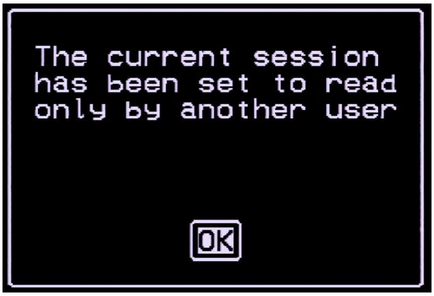
The menu presented to the connecting user and the notification messages to the previous user are as follows:



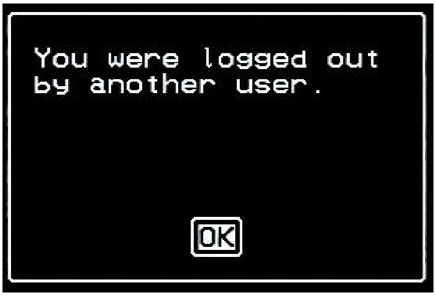
Server 3 (Port 3) - This port is connected to another station.



Another user connecting on this station



The current session has been set to read only by another user



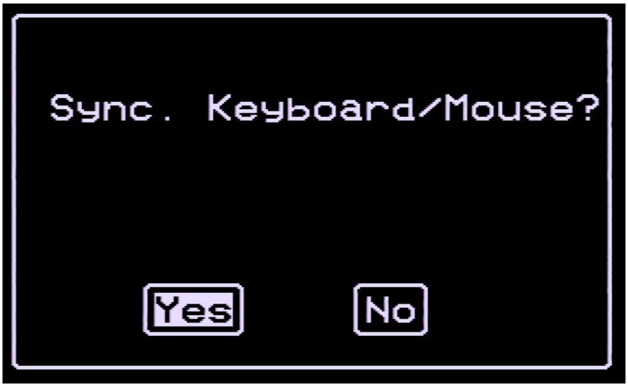
You were logged out by another user.

The connecting user is always granted the highest privilege mode based on its permission rights when the previous user is in read-only mode.

Once two users are connected to a server port, either user may choose at any time to change his/her access mode (or disconnect from the session by issuing a escape sequence command)

Synchronizing Your Keyboard and Mouse

There may be circumstances when your recently connected server do not support full operation of keyboard and mouse. To fix this, just issue a Keyboard/Mouse Sync command (default keys: Ctrl-K, and then S). This key sequence invokes the following confirmation window:



Sync. Keyboard/Mouse?

Select **Yes** to enable your keyboard and mouse again.

Establishing a Power Control Session

Power Control by Escape Sequence

If you have an AlterPath PM powering one or more computers connected to your KVM/net unit, you may initiate a power control session at any time once you are connected. You first connect to the desired computer by following the steps in the *Connecting to a Server* section of this chapter. Once connected, you can press, at any time, the power command key sequence (**Ctrl-K** then **P**, default).

Power Control Over IP

If you have Power Manager configured into the KVM/net switch, then you should be able to use the Power Management form of the web interface.

Power Management

Depending on your access rights, KVM/net allows you to remotely view and manage all Intelligent Power Distribution Units (IPDUs) connected to the KVM/net unit. Power management configuration comprises five tabbed forms, of which only the first two are available to the regular user:

Form Title	*Use this form to:*
Outlets Manager	Switch on/off and lock/unlock outlets; reboot network devices.
View IPDUs Info	View IPDU information by ports and slaves. The information form provides real-time, global, current monitoring of all connected devices.
Users Manager	*For admin user only.* This form is used to Add or delete users assigned to specific outlets.
Configuration	*For admin user only.* This form is used to enable over power protection, syslog and alarm notification from any specified port. The form allows the administrator to set a current alarm threshold that once exceeded will have the KVM/net sound an alarm or send a notification message.
Software Upgrade	*For admin user only.* This form is used to upgrade the AlterPath Power Manager software.

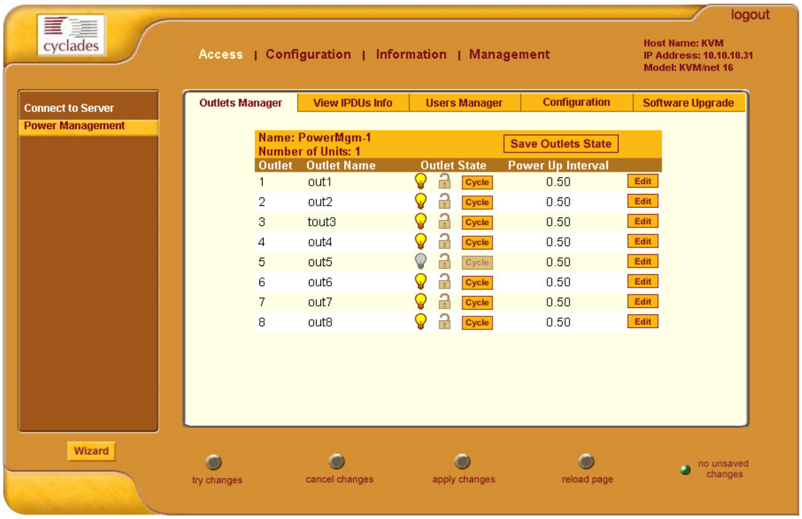
If you have admin privileges and you need to configure Power Management using the other tabbed forms, refer to **Chapter 3: KVM/net Configuration** for a detailed explanation of these forms.

Access > Power management > Outlets Manager

The **Outlets Manager** form allows you to check the status of all IPDUs connected to the Console Server, including their outlets. Any user who has Administration privileges can turn on, turn off, cycle, lock and unlock the outlets.

1. From the top menu, select **Access**; from the left menu, select **Power Management**.

   The system invokes the following form:



Host Name: KVM
IP Address: 10.10.10.31
Model: KVM/net 16

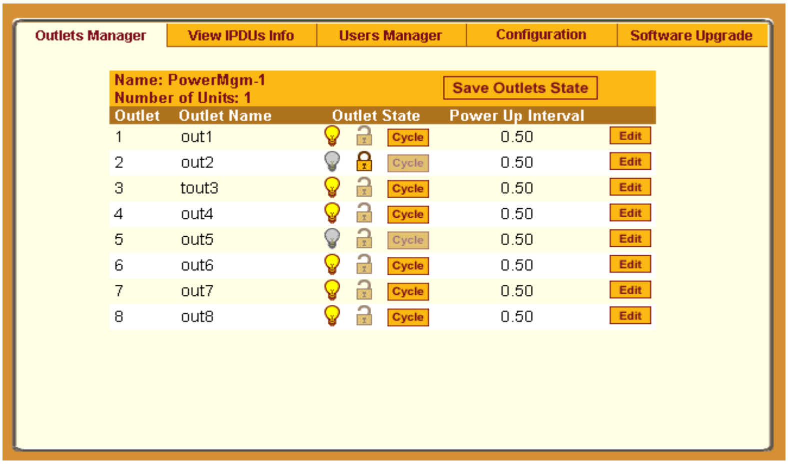
Name: PowerMgm-1
Number of Units: 1

Outlet	Outlet Name	Outlet State	Power Up Interval	
1	out1	Cycle	0.50	Edit
2	out2	Cycle	0.50	Edit
3	tout3	Cycle	0.50	Edit
4	out4	Cycle	0.50	Edit
5	out5	Cycle	0.50	Edit
6	out6	Cycle	0.50	Edit
7	out7	Cycle	0.50	Edit
8	out8	Cycle	0.50	Edit

   In the example above, the yellow bulbs (*i.e*, the actual color online when the switch is ON) and the opened padlock indicate that the outlets are switched on and unlocked.

2. To switch on/off an outlet, click on the light bulb; to lock/unlock an outlet, click on the padlock.

In the sample form below, outlet 2 is switched off and locked.



Name: PowerMgm-1
Number of Units: 1

Outlet	Outlet Name	Outlet State			Power Up Interval	
1	out1	●	🔓	Cycle	0.50	Edit
2	out2	○	🔒	Cycle	0.50	Edit
3	tout3	●	🔓	Cycle	0.50	Edit
4	out4	●	🔓	Cycle	0.50	Edit
5	out5	○	🔓	Cycle	0.50	Edit
6	out6	●	🔓	Cycle	0.50	Edit
7	out7	●	🔓	Cycle	0.50	Edit
8	out8	●	🔓	Cycle	0.50	Edit

3. To save your changes, click on the **Save Outlets State** button located in the form.
4. From the lower control buttons of the main window, click on the **Apply Changes** button.

Access > Power Management > View IPDUs Info

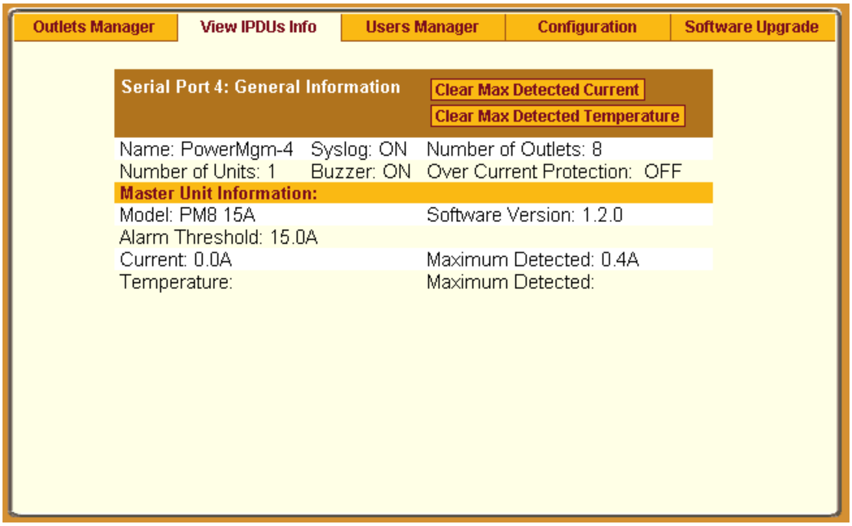
The IPDU Info form allows you to view all IPDU information (*e.g.*, number of outlets of each unit, current, temperature, alarm threshold levels, firmware, etc.) by serial port.

The form stores historical values of the maximum current and the maximum temperature.

To view IPDU information, perform the following steps:

1. From the top menu bar, select **Access**; from the left menu panel, select **Power Management**; from the form tabs, select **View IPDUs Info**.

   The system brings up the **IPDUs Info** form:



Serial Port 4: General Information

Name: PowerMgm-4 Syslog: ON Number of Outlets: 8
Number of Units: 1 Buzzer: ON Over Current Protection: OFF

Master Unit Information:

Model: PM8 15A Software Version: 1.2.0
Alarm Threshold: 15.0A
Current: 0.0A Maximum Detected: 0.4A
Temperature: Maximum Detected:

2. To delete the stored values for the maximum detected current, select the **Clear Max Detected Current** button.
3. To delete the stored values for the maximum detected temperature, select the **Clear Max Detected Temperature** button.

This page has been left intentionally blank.

Glossary

3DES

Derived from DES which is an acronym for Data Encryption Standard. DES was originally developed by IBM as Lucifer in the early 1970's. The NSA and NIST used a modified version of Lucifer and named it DES. DES was adopted as the federal standard in 1976 (FIPS (46-3) and ANSI standard X9.32).

However, DES became vulnerable as computers got more powerful and so NIST defined 3DES or Triple DES in 1999. 3DES uses three stages of DES so it is much more secure and suffices for most applications currently.

Advantages of 3DES:

It is easy to implement in both hardware and software compared to other algorithms.

It is based on DES which is a very trusted cipher. DES has been studied thoroughly for over 25 years now and is proven to have sound basics though the key length is too small now.

It is much faster than public key cryptography methods like the RSA method. (Source: www: 3DES and Encryption, Kenneth Castelino)

Authentication

The process by which a user’s identity is checked within the network to ensure that the user has access to the requested resources.

Basic In/Out System (BIOS)

Chips on the motherboard of a computer contain read only memory instructions that are used to start up a computer. The operating system of a PC also makes use of BIOS instructions and settings to access hardware components such as a disk drive. Some BIOS/CMOS settings can be set to scan for viruses, causing problems for some installation programs.

Baud Rate

The baud rate is a measure of the number of symbols (characters) transmitted per unit of time. Each symbol will normally consist of a number of bits, so the baud rate will only be the same as the bit rate when there is one bit per symbol. The term originated as a measure for the transmission of telegraph characters. It has little application today except in terms of modem operation. It is recommended that all data rates are referred to in bps, rather than baud (which is easy to misunderstand). Additionally, baud rate cannot be equated to bandwidth unless the number of bits per symbol is known.

Boot To start a computer so that it is ready to run programs for the user. A PC can be booted either by turning its power on, (Cold Boot) or by pressing Ctrl+Alt+Del (Warm Boot).

CAT-5 Category 5. A cabling standard for use on networks at speeds up to 100 Mbits including FDDI and 100base-T. The 5 refers to the number of turns per inch with which the cable is constructed.

Console Terminal used to configure network devices at boot (start-up) time. Also used to refer to the keyboard, video and mouse user interface to a server.

Checksum A computed value which depends on the contents of a block of data and which is transmitted or stored along with the data in order to detect corruption of the data. The receiving system recomputes the checksum based upon the received data and compares this value with the one sent with the data. If the two values are the same, the receiver has some confidence that the data was received correctly.

DHCP Dynamic Host Configuration Protocol. A protocol for automatic TCP/IP configuration that provides static and dynamic address allocation and management.

DHCP enables individual computers on an IP network to extract their configurations from a server (the 'DHCP server') or servers, in particular, servers that have no exact information about the individual computers until they request the information. The overall purpose of this is to reduce the work necessary to administer a large IP network. The most significant piece of information distributed in this manner is the IP address.

Escape Sequence

A sequence of special characters that sends a command to a device or program. Typically, an escape sequence begins with an escape character, but this is not universally true.

An escape sequence is commonly used when the computer and the peripheral have only a single channel in which to send information back and forth. If the device in question is "dumb" and can only do one thing with the information being sent to it (for instance, print it) then there is no need for an escape sequence. However most devices have more than one capability, and thus need some way to tell data from commands.

Ethernet

A LAN cable-and-access protocol that uses twisted-pair or coaxial cables and CSMA/CD (Carrier Sense Multiple Access with Collision Detection), a method for sharing devices over a common medium. Ethernet runs at 10 Mbps; Fast Ethernet runs at 100 Mbps. Ethernet is the most common type of LAN.

Flash

Flash refers to a type of memory that can be erased and reprogrammed in units of memory known as blocks rather than one byte at a time; thus, making updating to memory easier.

Flow Control

A method of controlling the amount of data that two devices exchange. In data communications, flow control prevents one modem from "flooding" the other with data. If data comes in faster than it can be processed, the receiving side stores the data in a buffer. When the buffer is nearly full, the receiving side signals the sending side to stop until the buffer has space again. Between hardware (such as your modem and your computer), hardware flow control is used; between modems, software flow control is used.

Hot-Swap

Ability to remove and add hardware to a computer system without powering off the system.

IP Address

A 32-bit address assigned to hosts using TCP/IP. It belongs to one of five classes (A-E) and is expressed as 4 octets separated by periods formatted as dotted decimals. Each address has a network number, an optional sub network number and a host number. The first two numbers are used for routing, while the host number addresses an individual host within the network or sub network. A subnet mask is used to extract network and sub network information from the IP address.

IP packet filtering

This is a set of facilities in network equipment that allows the filtering of data packets based on source/destination addresses, protocol, TCP port number and other parameters. Packet filtering is one of the main functions of a firewall.

IPsec

Short for *IP Security Protocol*, IPsec is an extended IP protocol that provides encrypted security services. These services enable authentication, as well as for access and trustwothiness control. IPsec provides similar services as SSL, but it works on a network layer. Through IPsec you can create encrypted tunnels (VPN) or encrypt traffic between two hosts.

Kerberos

Kerberos was created by MIT as a solution to network security problems. The Kerberos protocol uses strong cryptography so that a client can prove its identity to a server (and vice versa) across an insecure network connection. After a client and server has used Kerberos to prove their identity, they can also encrypt all of their communications to assure privacy and data integrity as they go about their business.

KVM

Keyboard, video and mouse interface to a server.

LDAP

Lightweight Directory Access Protocol. A software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the Internet or on a corporate intranet. LDAP is a "lightweight" (smaller amount of code) version of DAP (Directory Access Protocol), which is part of X.500, a standard for directory services in a network.

MAC

Medium Access Control. Internationally unique hardware identification address that is assigned to the NIC (Network Interface Card) which interfaces the node to the LAN.

Network Mask

A number used by software to separate the local subnet address from the rest of a given Internet protocol address

Network masks divide IP addresses into two parts (network address and address of a particular host within the network). Mask have the same form as IP addresses (i.e. 255.255.255.0), however, its value is needed to be understood as a 32-bit number with certain number of ones on the left end and zeros as the rest. The mask cannot have an arbitrary value. The primary function of a subnet mask is to define the number of IP hosts that participate in an IP subnet. Computers in the same IP subnet should not require a router for network communication.

NTP

Network Time Protocol. A standard for synchronizing your system clock with the ``true time", defined as the average of many high-accuracy clocks around the world.

OSD

On-Screen Display.

Packet

A packet is a basic communication data unit used when transmitting information from one computer to another. The maximum length of a packet depends on the communication medium. As an example, in Ethernet networks the maximum length is1500 bytes. A data packet can be divided into two parts: the header part and the data part. The header contains information needed for communication between nodes; the data is the body of the packet that is ultimately received by the application.

Parity

In serial communications, the parity bit is used in a simple error detection algorithm. As a stream of data bits is formed, an extra bit, called the parity bit, is added. This bit is set on (1) or off (0), depending on the serial communications parameters set in the UART chip.

The following lists the available parity parameters and their meanings:

Odd - Parity bit set so that there is an odd number of 1 bits
Even - Parity bit set so that there is an even number of 1 bits
None - Parity bit is ignored, value is indeterminate

Port

A port is a 16-bit number (the allowed range being 1 through 65535) used by the TCP and UDP protocols at the transport layer. Ports are used to address applications (services) that run on a computer. If there was only a single network application running on the computer, there would be no need for port numbers and the IP address only would suffice for addressing services. However, several applications may run at once on a particular computer and we need to differentiate among them. This is what port numbers are used for. Thus, a port number may be seen as an address of an application within the computer.

PPP

Point-to-Point Protocol. This protocol is a way to connect your computer to the Internet over telephone lines. PPP is replacing an older protocol, SLIP, as it is more stable and has more error-checking features.

PPP has been a widely-used Internet standard for sending datagrams over a communications link. The PPP standard is described in RFC 1661 by the Point-to-Point Working Group of the Internet Engineering Task Force (IETF). PPP is commonly used when remote computers call an Internet service provider (ISP) or a corporate server that is configured to receive incoming calls.

RADIUS

Remote Authentication Dial-In User Service) is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share.

SMTP

Simple Mail Transfer Protocol. Specifies the format of messages that an SMTP client on one computer can use to send electronic mail to an SMTP server on another computer.

SNMP

Short for *Simple Network Management Protocol*, a set of protocols for managing complex networks. The first versions of SNMP were developed in the early 80s. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network.

SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

(Source: Webopedia)

SNMP Traps

Notifications or Event Reports are occurrences of Events in a Managed system, sent to a list of managers configured to receive Events for that managed system. These Event Reports are called Traps in SNMP. The Traps provide the value of one or more instances of management information.

Any SNMP enabled Device generates Fault Reports (Traps) that are defined in the MIB (which the SNMP Agent has implemented).

The Trap Definition vary with the SNMP Version (which defines the messaging format), but the information contained in these are essentially identical. The major difference between the two message formats is in identifying the events.

SSH

Secure Shell. A protocol which permits secure remote access over a network from one computer to another. SSH negotiates and establishes an encrypted connection between an SSH client and an SSH server.

Stop Bit

A bit which signals the end of a unit of transmission on a serial line.A stop bit may be transmitted after the end of each byte or character.

Subnet Mask

A bit mask used to select bits from an Internet address for subnet addressing. Also known as Address Mask.

TACACS

Terminal Access Controller Access Control System.

Authentication protocol, developed by the DDN community, that provides remote access authentication and related services, such as event logging. User passwords are administered in a central database rather than in individual routers, providing an easily scalable network security solution.

TACACS+

Terminal Access Controller Access Control System Plus. A protocol that provides remote access authentication, authorization, and related accounting and logging services, used by Cisco Systems.

Telnet A terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on your computer and connects your PC to a server on the network. You can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console.

TTY 1. In Unix, refers to any terminal; sometimes used to refer to the particular terminal controlling a given job (it is also the name of a Unix command which outputs the name of the current controlling terminal). 2. Also in Unix, any serial port, whether or not the device connected to it is a terminal; so called because under Unix such devices have names of the form **tty**.

UDP *User Datagram Protocol* uses a special type of packet called a datagram. Datagrams do not require a response; they are one way only (connectionless). Datagrams are usually used for streaming media because an occasional packet loss will not affect the final product of the transmission.

VPN *Virtual Private Networking* allows local area networks to communicate across wide area networks, typically over an encrypted channel. See also: **IPsec**.